MODELO DE IMPLEMENTACION DE CIBERSEGURIDAD PARA SISTEMAS IOT EN EL MARCO DE REDES 5G

ALEXANDER DE JESÚS CELÍN BARRAZA

Universidad Tecnológica de Pereira
Facultad de Ingenierías
Pereira, Colombia
2019

MODELO DE IMPLEMENTACION DE CIBERSEGURIDAD PARA SISTEMAS IOT EN EL MARCO DE REDES 5G

ALEXANDER DE JESÚS CELÍN BARRAZA

Proyecto de grado presentado como requisito parcial para optar al título de:
Magister en Ingeniería de Sistemas y Computación

Director:
MSc. Cesar Augusto Jaramillo Acevedo

Universidad Tecnológica de Pereira
Facultad de Ingenierías
Pereira, Colombia
2019

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

FIRMA DIRECTOR

_____

FIRMA JURADO

_____

FIRMA JURADO

Pereira, Risaralda, noviembre 2019

Dedicatoria

A mis Geniales padres Nidia y Alfredo, quienes con su constante aliento han forjado en su hijo favorito Alexander fortaleza para lograr lo que soy hoy.

A mi Amada esposa Norma Lucía por su permanente motivación y apoyo incondicional, así como a mis hijos Melissa y Stefania, Marcela y Santiago, quienes con su amor y paciencia alentaron este gran logro que hoy culmina con mucha satisfacción.

Agradecimientos

Dios, gracias que en todo momento estamos juntos y no me desamparas, que permitiste adicionar un nuevo logro a mi vida.

A los ingenieros Jorge Iván Ríos por su gran aporte en el proceso y apoyo desinteresado; y Cesar Augusto Jaramillo Acevedo por su valioso acompañamiento como director.

Por último, pero no menos importante a nuestros docentes y compañeros Luisa Fernanda Ríos Alzate, José Arbey Vanegas Camargo, Luis Gerardo Borja Sánchez, entre otros, con quienes gratamente compartí esta gran experiencia de crecimiento personal y valioso aprendizaje.

Resumen

Internet de las cosas (IoT) es una tecnología cada vez más popular que es utilizada ampliamente en la producción industrial y en aplicaciones sociales, como hogares inteligentes, atención médica y automatización industrial. Si bien IoT puede ser una tecnología económica y socialmente beneficiosa, su implementación plantea dificultades, riesgos y problemas de seguridad que deben tomarse en consideración. Por lo general, IoT tiene una arquitectura de tres capas que consiste en capas de Percepción, Red y Aplicación. Se deben aplicar varios principios de seguridad en cada capa para lograr un entorno IoT seguro. A su vez, es necesario para IoT correr sobre una tecnología que pueda soportar grandes cantidades de transmisión de datos de manera eficiente y con un ancho de banda muy alto. En un futuro próximo, es decir, los dispositivos IOT de próxima generación, algunos de los principales objetivos o demandas que deben abordarse son el aumento de la capacidad, la mejora de la velocidad de datos y la disminución de la latencia, el desarrollo de la tecnología de comunicación móvil inalámbrica de próxima generación, a saber, 5G, que promete satisfacer las necesidades de arquitecturas IOT complejas. Para comprender mejor las razones esenciales de las nuevas amenazas de IoT y los desafíos en la investigación actual, este trabajo presenta una descripción general de los principios de seguridad, los desafíos tecnológicos, las contramedidas propuestas y las orientaciones futuras en el IoT, finalmente se presenta un modelo conceptual como marco de ejecución para la implementación de ciber seguridad en entornos IoT.

Abstract

Internet of things (IoT) is an increasingly popular technology that is widely used in industrial production and social applications, such as smart homes, medical care, and industrial automation. While IoT can be an economically and socially beneficial technology, its implementation poses difficulties, risks and security problems that must be taken into consideration. In general, IoT has a three-layer architecture consisting of

Perception, Network and Application layers. Several security principles must be applied at each layer to achieve a secure IoT environment. At the same time, it’s necessary for IoT to run on a technology that can support great quantities of data transmission efficiently and with a very high bandwidth. In the near future, that is, next-generation IOT devices, some of the main objectives or demands that must be addressed are the increase in capacity, the improvement of data speed and the latency decrease, the development of Next generation wireless mobile communication technology, namely 5G, which promises to meet the complex IOT architecture needs. To better understand the essential reasons for the new IoT threats and the challenges in current research, this paper presents a general description of security principles, technological challenges, the proposed countermeasures and future orientations in the IoT, Finally, a conceptual model is presented as the execution framework for the implementation of cyber security in IoT environments.

Contenido

Índice de imágenes

Índice de tablas

Capítulo I: Marco teórico

1.1 Definiciones

Internet de las cosas (IoT) es una tecnología cada vez más popular de muchos objetos, servicios, personas y dispositivos interconectados que pueden comunicarse, compartir datos e información para lograr un objetivo común en diferentes dominios de implementación. Algunas aplicaciones de IoT son definidas en (Mosenia & Jha, 2017) así:

- Edificios inteligentes: los hogares y edificios inteligentes permiten una gestión energética eficaz. Por ejemplo, los termostatos inteligentes, que tienen sensores integrados y algoritmos de análisis de datos, pueden controlar los aires acondicionados según las preferencias y hábitos del usuario. Además, los controladores inteligentes pueden ajustar la iluminación según el uso del usuario. Varios artículos para el hogar, por ejemplo, refrigeradores, televisores y sistemas de seguridad, podrían tener sus propias unidades de procesamiento y proporcionar servicios a través de Internet. Estos dispositivos inteligentes mejoran en gran medida la comodidad de los usuarios. Los dispositivos controlables de forma remota reciben comandos de los usuarios para realizar acciones que tienen un efecto en el entorno circundante.
- Gestión de energía: el uso de sistemas inteligentes basados en IoT, que integran sensores integrados y componentes de actuación, permite un enfoque proactivo para optimizar el consumo de energía. En particular, se espera que las tomas de corriente, lámparas, refrigeradores y televisores inteligentes, que se pueden controlar de forma remota, compartan información con las empresas de suministro de energía para optimizar el consumo de energía en los hogares inteligentes. Además, tales cosas permiten a los

usuarios controlarlos o administrarlos de forma remota, y permiten una programación que puede conducir a una reducción significativa en el consumo de energía.

- Gestión de la construcción: el monitoreo y la gestión de la infraestructura moderna, por ejemplo, puentes, semáforos, vías férreas y edificios, son una de las aplicaciones clave de IoT, puede usarse para monitorear cualquier cambio repentino en las condiciones estructurales que pueda conducir a riesgos de seguridad.
- Monitoreo ambiental: el uso de elementos inteligentes con sensores integrados permite el monitoreo ambiental y la detección de situaciones de emergencia, por ejemplo, una inundación, que requieren una respuesta rápida. Además, la calidad del aire, la humedad, la temperatura y el agua pueden ser examinadas por dispositivos basados en IoT.

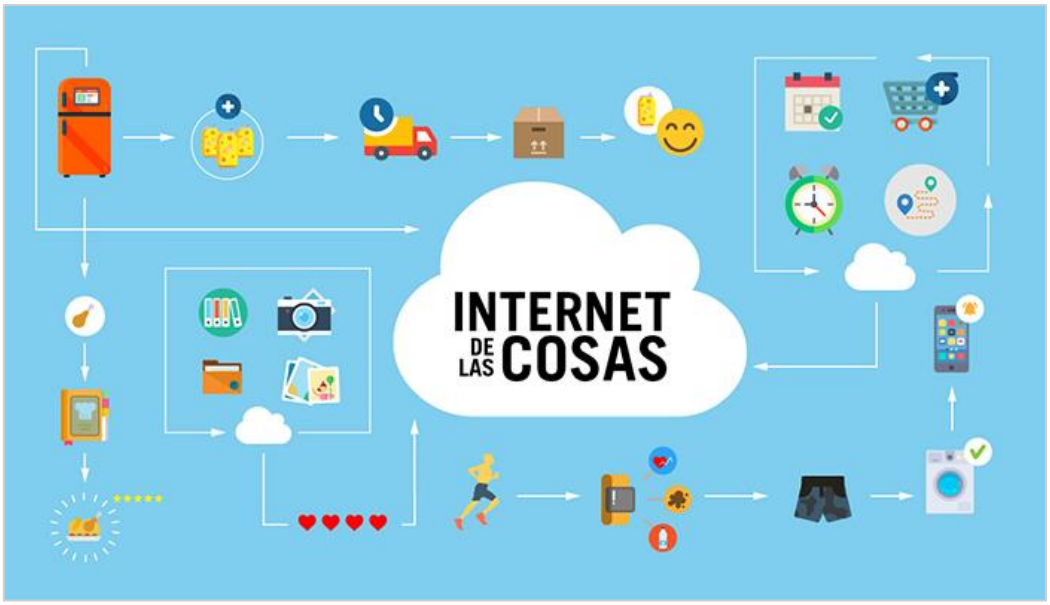

Figura 1 Internet de las cosas
(Fuente: https://www.bymovil.com/que-es-el-internet-de-las-cosas/)

También se implementa en la agricultura, vehículos inteligentes, monitoreo de la salud, gestión de la línea de producción y montaje, cadena de suministro de alimentos. Estas son solo algunas de las instancias de IoT.

La Unión Internacional de Telecomunicaciones (UIT, 2012) organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), define IoT como una infraestructura global para la Sociedad de la Información, permitiendo servicios avanzados mediante la interconexión de cosas (físicas y virtuales) basadas en tecnologías de información y comunicación interoperables existentes y en evolución.

Otras definiciones de IoT son abordadas por (Andrés, 2018) manifestando en su libro que el término Internet de las Cosas (IoT) fue acuñado por primera vez por el pionero de la tecnología británica Kevin Ashton en una presentación que realizó en 1999 para la multinacional Procter & Gamble, donde describía un sistema en el cual los objetos en el mundo físico podrían conectarse a Internet a través de sensores para automatizar la recogida de datos, propugnando su aplicación en la cadena de suministro añadiéndoles etiquetas RFID.

Del mismo autor y texto, se extrae que los autores HALLER, KARNOUSKOS y SCHIROTH conceptúan IoT como "un mundo donde los objetos físicos se integran perfectamente en la red de información y donde los objetos físicos pueden convertirse en participantes activos en los procesos empresariales. Los servicios están disponibles para interactuar con estos «objetos inteligentes» a través de Internet, consultar su estado y cualquier información asociada con ellos, teniendo en cuenta las cuestiones de seguridad y privacidad".

1.2 Crecimiento de IoT

Según la firma de investigación **Gartner**, en el año 2017 se conectaron 8.400 millones de dispositivos, un 31% más que en 2016 y la enorme cifra de 20.415 millones de dispositivos

estarían habilitados para el próximo año 2020 (Gartner, 2017). Por su parte, el proveedor líder de datos de mercado e información sobre los consumidores **Statista** afirma que la cantidad de dispositivos conectados en todo el mundo aumentará dramáticamente de 20.35 billones en 2017 a 75.44 billones en 2025 (Statista, 2016). De otra parte, International Data Corporation predijo una tasa de crecimiento anual compuesta de 17% en el gasto de IoT: 1.3 billones en 2019 (Ironpaper, 2016), de todo lo anterior se percibe hay un consenso que el impacto de las tecnologías de IoT es sustancial y creciente.

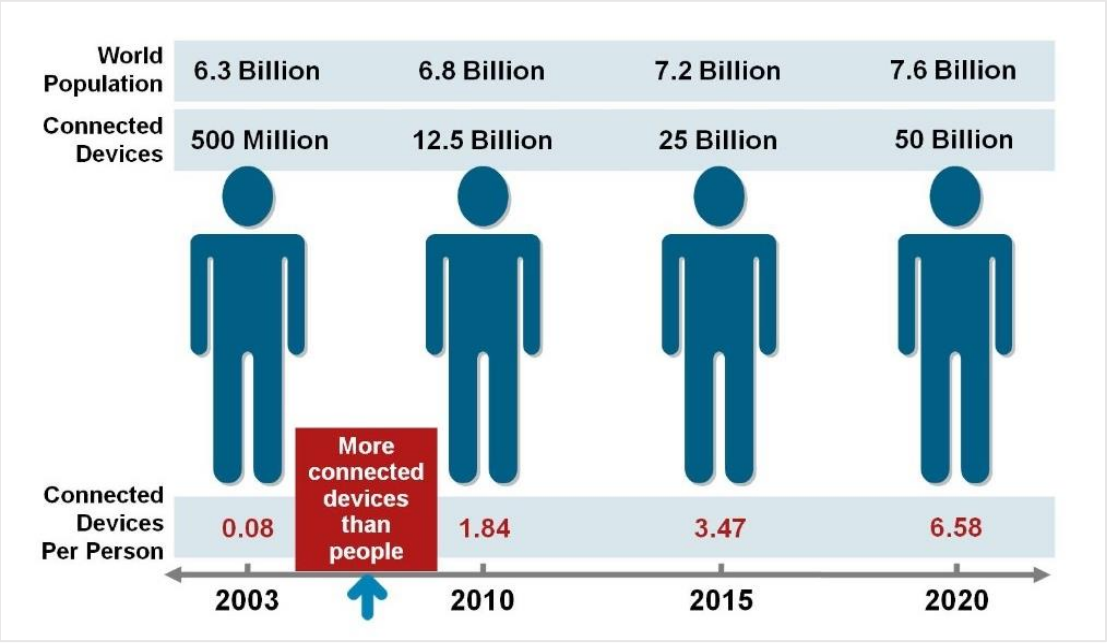

Figura 2 Predicción para el mercado de IoT
(Fuente Cisco IBSG, abril 2011)

1.3 Arquitectura IoT

IoT es una de las innovaciones destacadas que tiene el potencial de proporcionar beneficios ilimitados, el desarrollo de la IoT está a punto de alcanzar una etapa en la que muchos de los objetos que nos rodean tendrán la capacidad de conectarse a Internet para comunicarse entre sí

sin intervención humana. Originalmente, la IoT pretendía reducir los esfuerzos de ingreso de datos y utilizar diferentes tipos de sensores para recopilar esa información del entorno y permitir su almacenamiento y procesamiento automático, los cuales son generados en volumen, variedad y velocidad a un ritmo acelerado, para el cual los modelos de hoy no están diseñados. La transferencia de todos los datos de los nodos a la nube para su análisis y monitoreo de manera segura y eficiente requeriría una gran cantidad de ancho de banda, por lo tanto, el manejo de este volumen, variedad y velocidad de datos IoT requiere un nuevo modelo informático. IoT es una tecnología que aún está en desarrollo y necesita muchas mejoras a un nivel diferente. La arquitectura de IoT aborda factores esenciales como la calidad de servicio (QoS), y los requisitos de seguridad que tradicionalmente se dividen en tres categorías principales:

La ***Confidencialidad*** de los datos se refiere a la capacidad de garantizar la privacidad del usuario al proporcionar una conexión segura solo a los usuarios permitidos. Solo el usuario autorizado puede acceder a los datos. La confidencialidad de los datos se puede lograr mediante un mecanismo de encriptación de datos donde cada bit de datos se convierte en texto cifrado y seguido por un proceso de verificación de dos pasos, en el que dos dispositivos / componentes permiten el acceso solo si ambos dispositivos pasan la prueba de autenticación.

La ***Integridad*** de los datos consiste en que la manipulación de datos no se pueda realizar sin que el sistema detecte la amenaza. La suma de verificación y la verificación de redundancia cíclica son algunos métodos de detección de errores utilizados para verificar la integridad de los datos.

El objetivo principal de un sistema IoT consiste en proporcionar los datos a sus usuarios, siempre que sea necesario. El acceso inmediato a los datos por parte de su usuario no solo en condiciones normales sino también en condiciones desastrosas debería ser posible. Los firewalls se incorporan a la red para contrarrestar los ataques a los servicios, como el ataque de denegación de servicio, que puede negar la ***Disponibilidad*** de los datos al usuario final.

Existen diferentes opiniones con respecto al número de capas en un sistema IoT. Los autores (Tuwanut, 2016) afirman que IoT opera principalmente en tres capas denominadas Capa de Red, Capa de Percepción y Capa de Aplicación; y que cada capa IoT tiene problemas de seguridad inherentes asociados con ella. La Figura 1, página 2, muestra el marco arquitectónico básico de tres capas de IoT con respecto a los dispositivos y tecnologías que abarcan cada capa.

La capa de ***Percepción*** también se conoce como la capa sensores, el propósito de esta capa es adquirir los datos del entorno con la ayuda de sensores y actuadores como etiquetas RFID, código de respuesta rápida (QR), etc. Esta capa detecta, recopila y procesa información y luego la transmite a la capa de red, también realiza la colaboración del nodo IoT en redes locales y de corto alcance.

La capa de ***Red*** cumple la función de enrutamiento y transmisión de datos a diferentes hubs y dispositivos IoT a través de Internet. En esta capa, las plataformas de computación en la nube, las puertas de enlace de Internet, los dispositivos de conmutación y enrutamiento, etc. funcionan utilizando algunas de las tecnologías más recientes, como WiFi, LTE, Bluetooth, 3G, Zigbee, etc. Las puertas de enlace de la red sirven como mediador entre diferentes IoT nodos mediante

la agregación, el filtrado y la transmisión de datos hacia y desde diferentes sensores y mantiene confidencial la información de los dispositivos y sensores.

La capa de ***Aplicación*** es el proveedor de servicios para el usuario final. Dado que esta capa es la puerta hacia internet, pueden surgir numerosas amenazas. Este nivel garantiza la autenticación del usuario y el acceso a datos personales y confidenciales; por lo tanto, el protocolo debe proporcionar mecanismos para evitar que intrusos y usuarios malintencionados accedan al sistema. Los ataques tradicionales pueden ocurrir: ataques DDoS, falsificación, modificación de datos, escuchas ilegales, etc. El objetivo de la IoT de desarrollar un entorno inteligente que se lograría en la capa de aplicación.

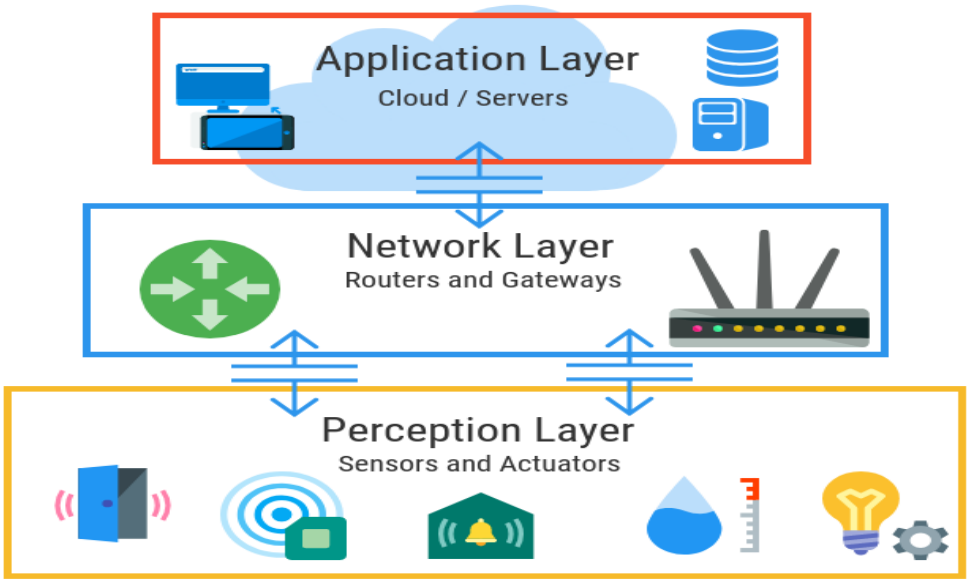

Figura 3 Arquitectura fundamental de tres capas de IoT
(Fuente: https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/)

1.4 Seguridad en IoT

Los objetivos de seguridad típicos de confidencialidad, integridad y disponibilidad (CIA) también se aplican a IoT. Sin embargo, IoT tiene muchas restricciones y limitaciones en cuanto a los componentes y dispositivos, los recursos computacionales y de energía, e incluso la naturaleza heterogénea y ubicua de IoT que introduce preocupaciones adicionales.

1.4.1 Protocolos

En informática y telecomunicaciones, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema se comuniquen entre ellas para transmitir información. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

Figura 4 Esquema básico de un protocolo de comunicaciones
(Fuente: https://aprendiendoarduino.wordpress.com/2018/11/17/protocolos-iot-capa-aplicacion/)

En cuanto a los protocolos IoT más utilizados, (INCIBE, 2019) hace una descripción de ellos resumiéndose así:

Protocolos de entorno doméstico.

- ✓ **AllJoyn:** fue lanzado por The AllSeen Alliance, compuesta por Haier, LG, Microsoft, Panasonic, Qualcomm, Sharp, Silicon Image, Technicolor y TP-Link. Es un estándar de

código abierto, que facilita la comunicación entre dispositivos y aplicaciones, para todo tipo de protocolos de la capa de transporte.

- ✓ **HomePlug y HomeGrid:** son protocolos cuya comunicación se realiza a través de la red eléctrica. Esta tecnología de comunicación la implementan numerosas marcas. Dependiendo del producto adquirido, el tipo de cifrado es diferente, incluso algunos dispositivos transmiten la información sin cifrar.
- ✓ **MFi (Made For iPhone/iPod/iPad):** es un protocolo de comunicaciones propio de Apple diseñado para interactuar con estos dispositivos. Los dispositivos y elementos de conexión de Apple incorporan un chip mediante el cual verifican que tanto los dispositivos, como los cables de conexión son originales.
- ✓ **OCF (Open Connectivity Foundation):** es un protocolo impulsado por Samsung, Intel, Microsoft, Qualcomm, Electrolux entre otras. Es un proyecto de código abierto que ofrece interconectividad con la filosofía just-works. Este protocolo pretende garantizar la interoperabilidad de millones de dispositivos, gracias a una implementación de referencia (IoTivity) y un programa de certificación.
- ✓ **Thread (network protocol)**: fue creado por el conjunto de empresas denominado Thread Group. Es una tecnología basada en las comunicaciones por red mediante IPv6 que utiliza cifrado AES. Por ello y por la flexibilidad que ofrece, es un protocolo muy seguro y está preparado para el futuro.

Protocolos de entorno industrial.

- ✓ **AMQP (Advanced Message Queuing Protocol):** es un protocolo del nivel 7 del modelo OSI (Capa Aplicación) para aplicaciones distribuidas que soporta

comunicaciones punto-a-punto y de tipo publicación / suscripción. Proviene del sector de servicios financieros y tiene presencia en el ámbito de TI y en el sector industria, siendo bastante limitada en este último. Ofrece un modelo robusto de comunicaciones que soporta transacciones y puede garantizarlas de forma completa. Ofrece seguridad a través de la autenticación y cifrado mediante SASL o TLS.

- ✓ **CoAP (Constrained Application Protocol)**: fue creado por IETF (Internet Engineering Task Force) para proveer la compatibilidad de HTTP con una mínima carga. Es un protocolo cliente / servidor, es similar a HTTP pero usa UDP / multicast en lugar de TCP, además de simplificar el encabezado reduce el tamaño de cada requerimiento. Desde el punto de vista de la seguridad utiliza DTLS (Datagram Transport Layer Security), que básicamente consiste en aplicar seguridad en la capa de transporte para proteger las comunicaciones.
- ✓ **DDS (Data Distribution Service):** es un protocolo de tipo publicación/suscripción concebido para sistemas de tiempo-real. Es un estándar abierto y descentralizado. Los nodos de DDS se comunican directamente punto a punto a través de UDP/multidifusión (multicast). DDS es una buena solución para aplicaciones que requieren intercambio de datos en tiempo real como el control del tráfico aéreo, gestión de redes inteligentes, vehículos autónomos, robótica, sistemas de transporte, generación de electricidad, etc. Ofrece seguridad a través de TLS, DTSL y DDS.
- ✓ **HTTP (REST/JSON) (Hypertext Transfer Protocol):** es un protocolo cliente / servidor sin conexión presente en las TIC y en la web. Es un protocolo muy accesible por ser de código abierto, además de poseer numerosas librerías. Es efectivo para enviar grandes cantidades de información, como por ejemplo lecturas de sensores

minuto a minuto o cada hora; aunque no es adecuado ni para enviar actualizaciones en periodos de tiempo del orden de milisegundos ni para enviar información de video. Es muy recomendable asegurar la información transmitida aplicando el protocolo criptográfico SSL / TLS sobre HTTP, lo que genera el protocolo de aplicación HTTPS. No obstante, el método más seguro consiste en incluir en el dispositivo IoT solo un cliente HTTP, no un servidor HTTP, de manera que el dispositivo IoT pueda iniciar conexiones a un servidor web, pero no sea capaz de recibir solicitudes de conexión.

- ✓ **MQTT (Message Queuing Telemetry Transport):** es un protocolo de tipo publicación / suscripción de nivel de aplicación con una versión para redes no basadas en TCP / IP (p. ej. Zigbee) denominada MQTT-SN. Este protocolo ha sido implementado en múltiples aplicaciones de IT, IoT y OT, como, el Messenger de Facebook, MS Azure IoT hub o para entornos de generación de electricidad mediante fuentes renovables. Puesto que MQTT envía credenciales de conexión en claro y no incluye en su diseño medidas de seguridad (p. ej. autenticación o cifrado) es recomendable usarlo con TLS para asegurar las comunicaciones en su versión sobre TCP, así como los mecanismos propios compatibles de comunicaciones no basadas en TCP/IP.
- ✓ **OPC UA (Unified Architecture):** es un estándar de nueva generación que surge a partir del OPC, el cual es conocido por proveer una interfaz estándar para comunicarse con los PLC. OPC UA es un protocolo cliente / servidor multiplataforma, donde los clientes se conectan, navegan, leen y escriben al equipamiento industrial. Ofrece un modo binario y otro basado en SOAP (Web Service). Las tecnologías y metodologías

innovadoras, como los nuevos protocolos de transporte, los algoritmos de seguridad, los estándares de codificación o los servicios de aplicación pueden incorporarse en OPC UA mientras se mantiene la compatibilidad retroactiva para los productos existentes. Es una opción para conectar información de sensores y PLC en las aplicaciones industriales existentes como sistemas MES (Manufacturing Execution System) y SCADA (Supervisory Control And Data Acquisition). Este estándar implementa medidas de seguridad para las comunicaciones, como son autenticación de la aplicación, autenticación y autorización del usuario, disponibilidad del servidor, auditabilidad del sistema y confidencialidad e integridad, lo que lo convierte en un protocolo muy seguro. OPC UA ofrece seguridad nativa que incluye autenticación y autorización, cifrado e integridad de datos vía firmas. Para la versión SOAP hace uso de la especificación de seguridad para Web Service desarrollada por IBM, WS-SecureConversation, mientras que en la versión binaria hace uso de una implementación específica de la anterior. Soporta certificados X.509 para la autenticación y se puede integrar con directorio activo y PKI.

- ✓ **XMPP (Extensible Messaging and Presence Protocol):** es un protocolo abierto, escalable y descentralizado basado en XML, originalmente diseñado para mensajería instantánea. Las características de XML en cuanto a adaptabilidad y sencillez de XML han sido heredadas por el protocolo XMPP. Los servidores que utilizan este protocolo pueden estar aislados de la red pública XMPP, y poseen robustos sistemas de seguridad como SASL y TLS. Gran parte de los cortafuegos están configurados para permitir el trafico TCP del puerto utilizado por HTTP, pero bloquean el puerto

utilizado por XMPP, para solucionarlo XMPP utiliza HTTP para permitir el acceso a los usuarios que se encuentran tras un firewall.

	Transporte	Modelo	Ámbito de aplicación	Conocimiento del contenido	Datos principales	Seguridad	Prioridad de los datos	Tolerancia a fallos
AMQP	TCP/IP	Intercambio de mensajes punto a punto	D2D D2C C2C	Ninguno	Codificados	TLS	Ninguno	Específica de la implementación
CoAP	UDP/IP	Petición/Respuesta (REST)	D2D	Ninguno	Codificados	DTLS	Ninguno	Descentralizado
DDS	UDP/IP (unicast + mcast) TCP/IP	Publicación/Suscripción Petición/Respuesta	D2D D2C C2C	Enrutamiento basado en el contenido, consultas	Declarados codificados	TLS, DTLS, DDS	Prioridades de transporte	Descentralizado
MQTT	TCP/IP	Publicación/Suscripción	D2C	Ninguno	No definidos	TLS	Ninguno	El nodo central (broker) es el punto único de fallo (SPoF)

Tabla 1 Comparativa sobre algunos de los protocolos IoT
(Fuente: https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones)

La mayoría de los ataques no están dirigidos directamente a los actuadores o dispositivos, sino a los protocolos de comunicación (Department for Digital Culture) que se utilizan para transmitir los datos recopilados del dispositivo al hardware de almacenamiento y las herramientas de procesamiento. Es muy probable que esta transmisión se vea afectada por los ataques Man-in-the-Middle (MitM) o Denial-of-Service (DoS). Los protocolos de comunicación defectuosos en una base de datos incompleta pueden provocar la denegación del dispositivo o ataques de falta de sueño que agotan las baterías.

Entre los ataques conocidos más comunes en protocolos IoT tenemos el Ataque por fuerza bruta, Ataques por denegación de servicio, Utilización como plataforma de ataque hacia otros dispositivos y Ataque para obtención de datos.

1.4.2 Cifrado

Los dispositivos de IoT son generalmente inalámbricos y pueden estar ubicados en lugares públicos. La comunicación inalámbrica en Internet de hoy se hace más segura a través del cifrado. El cifrado también se considera clave para garantizar la seguridad de la información en IoT. Sin embargo, muchos dispositivos IoT actualmente no son lo suficientemente potentes como para admitir un cifrado sólido. Para habilitar el cifrado en la IoT, los algoritmos deben hacerse más eficientes y consumir menos energía, y se necesitan esquemas de distribución de claves eficientes.

Además del cifrado, la administración de identidades es un componente importante de cualquier modelo de seguridad y los identificadores únicos son esenciales para los dispositivos IoT. Estos identificadores pueden usarse para establecer identidades personales en instituciones financieras, identificar actividades ilegales y otras funciones. Por lo tanto, garantizar que los objetos inteligentes sean quienes dicen que son es esencial para el éxito de IoT.

Como IoT se caracteriza por cálculos limitados en términos de capacidad de procesamiento y almacenamiento, tiene aspectos a solucionar, como el rendimiento, la seguridad, la privacidad y la confiabilidad.

1.4.3 Latencia

Los datos de los dispositivos de IoT se envían a la nube a través de Internet para su procesamiento o almacenamiento. Dado que actualmente la velocidad de transferencia de datos de Internet no es tan rápida como se desea para algunas aplicaciones en tiempo real la respuesta a

la solicitud enviada desde el dispositivo de Cloud a IoT lleva algún tiempo, lo que no es aceptable en aplicaciones sensibles a la latencia. Los autores (Goswami, 2013) afirmaron que informáticos en la Universidad de California, Berkeley, han medido el costo de enviar 10 terabytes de datos desde el Área de la Bahía a Amazon en Seattle. En un enlace de internet de ancho de banda promedio, lleva casi 45 días transmitir este gran volumen de datos con un costo de USD $ 1,000 como transferencia de red cuota. Por otro lado, envío de diez discos de 1 terabyte a través de cualquier servicio de envío estándar tarda 1 día y cuesta USD $ 400 solamente, Por lo tanto, la computación en la nube no es adecuado para enviar grandes volúmenes de datos.

Para manejar y procesar el tiempo real o cualquier otra aplicación sensible a la latencia, se requiere minimizar esta latencia de transmisión para evitar cualquier pérdida de información y para operar efectivamente en tiempo real.

1.5 Seguridad de los datos

La seguridad de los datos de IoT es la principal preocupación, ya sea en el tránsito de IoT o incluso en reposo. Enviar datos a la nube para almacenamiento significa entregarlos a cualquier proveedor de servicios de terceros. Además, el almacenamiento de datos en el backend puede atraer a los hackers y es propenso a ataques externos. Por lo tanto, requiere monitoreo constante y se debe generar una respuesta automatizada a lo largo de un eventual ataque.

El autor Rolf H. (Weber, 2015) afirma que el desafío principal en el contexto de IoT es un desafío de privacidad y seguridad. En el futuro, IoT enfrentará el desafío de recopilar gran cantidad de datos y mantener su seguridad. Para esto se deben desarrollar tecnologías sólidas que

se ocupen de la seguridad en la comunicación y el almacenamiento de los datos. Se espera hacer mucho trabajo para resolver los problemas de seguridad y privacidad en IoT. Pero estas cuestiones con respecto a los datos de IoT han permanecido sin resolver. También se espera mucho trabajo para crear estándares de la industria que mantengan el nivel mínimo de privacidad. En caso de transmisión o almacenamiento de datos sensibles, por ejemplo, datos relacionados con la salud, información financiera o algunos datos críticos de defensa o datos confidenciales.

1.6 Aumento del ataque DDoS

Según el informe de análisis de datos sobre los ataques DDoS en el tercer trimestre de 2014, que fue anunciado recientemente por (Akami, 2014), los volúmenes de tráfico aumentaron significativamente a partir del tercer trimestre de 2013 y el nuevo tipo de ataque DDoS se ha renovado. En general, los ataques que utilizan la capa basada en el protocolo UDP o SYN están aumentando, y la tasa de ocurrencia es de ~ 72 millones de paquetes por segundo.

Además, recientemente se ha identificado un ataque de amplificación de protocolo de descubrimiento de servicio simple (SSDP) y se sabe que afecta a televisores inteligentes, cámaras inteligentes, etc. Por lo tanto, se espera que aumente la amenaza de un ataque DDoS a gran escala en un entorno de IoT.

1.7 Acceso no autorizado

Un marco de IoT puede proporcionar servicios mediante la recopilación de datos generados desde diferentes dispositivos sensores y procesándolos en datos valiosos. Alternativamente, los

propios dispositivos sensores pueden recopilar datos y proporcionar servicios. En tal entorno, existe una amenaza de fuga de datos y falsificación de datos por parte de los usuarios que acceden a los datos sin permiso.

1.8 Confidencialidad

Es muy importante asegurarse de que los datos estén seguros y solo estén disponibles para los usuarios autorizados. En IoT, un usuario puede ser humano, máquinas y servicios, objetos internos (dispositivos que forman parte de la red) y objetos externos (dispositivos que no forman parte de la red). Por ejemplo, es crucial asegurarse de que los sensores no revelen los datos recopilados a los nodos vecinos. Otro problema de confidencialidad que debe abordarse es cómo se gestionarán los datos. Es importante que los usuarios de IoT estén al tanto de los mecanismos de gestión de datos que se aplicarán, el proceso o la persona responsable de la gestión, y garantizar que los datos estén protegidos durante todo el proceso.

1.9 Integridad

El IoT se basa en el intercambio de datos entre muchos dispositivos diferentes, por lo que es muy importante garantizar la exactitud de los datos; que proviene del remitente correcto, así como para garantizar que los datos no se manipulen durante el proceso de transmisión debido a interferencias intencionadas o no intencionadas. La función de integridad se puede imponer manteniendo la seguridad de extremo a extremo en la comunicación de IoT. El tráfico de datos se administra mediante el uso de firewalls y protocolos, pero no garantiza la seguridad en los puntos finales debido a la naturaleza característica de la baja potencia de cómputo en los nodos de IoT.

1.10 Disponibilidad

La visión de IoT es conectar tantos dispositivos inteligentes como sea posible. Los usuarios de IoT deben tener todos los datos disponibles cuando lo necesiten. Sin embargo, los datos no son el único componente que se utiliza en la IoT; los dispositivos y servicios también deben estar disponibles cuando se necesiten de manera oportuna para alcanzar las expectativas de IoT.

1.11 Modelos IoT: Fog / Edge / Cloud

Como la IoT se caracteriza por cálculos limitados en términos de capacidad de procesamiento y almacenamiento, tiene muchos problemas, como el rendimiento, la seguridad y la CIA. La integración de IoT con la nube, conocida como Cloud of Things (CoT), es la forma correcta de superar la mayoría de estos problemas (Atlam, Alenezi, Alharthi, Walters, & Wills, 2018). El CoT simplifica el flujo de recolección y procesamiento de datos de IoT y proporciona una instalación e integración rápidas y de bajo costo para el procesamiento y despliegue de datos complejos.

1.12 Fog Computing

La integración de IoT con la computación en la nube brinda muchas ventajas a diferentes aplicaciones de IoT. Sin embargo, como hay una gran cantidad de dispositivos IoT con plataformas heterogéneas, el desarrollo de nuevas aplicaciones IoT es una tarea difícil. Esto se debe a que las aplicaciones de IoT generan grandes cantidades de datos de sensores y otros dispositivos. Estos grandes datos se analizan posteriormente para determinar las decisiones con respecto a diversas acciones. Enviar todos estos datos a la nube requiere un ancho de banda de red excesivamente alto. Para superar estos problemas, la computación de niebla entra en juego.

El término computación de niebla fue acuñado por Cisco (F Bonomi, 2012). Es una nueva tecnología que proporciona muchos beneficios a diferentes campos, especialmente el IoT. Similar a la nube, la computación en niebla proporciona servicios a los usuarios de IoT, como el procesamiento y almacenamiento de datos. La computación de niebla se basa en proporcionar capacidades de procesamiento de datos y almacenamiento local a dispositivos de niebla en lugar de enviarlos a la nube.

El propósito de la computación en niebla en IoT es mejorar la eficiencia, el rendimiento y reducir la cantidad de datos transferidos a la nube para su procesamiento, análisis y almacenamiento. Por lo tanto, los datos recopilados por los sensores se enviarán a los dispositivos periféricos de la red para su procesamiento y almacenamiento temporal, en lugar de enviarlos a la nube, reduciendo así el tráfico y la latencia de la red.

Esencialmente, la computación en niebla es una extensión de la nube, pero más cercana a las cosas que funcionan con los datos de IoT. Como se muestra en la Figura 5, página 20, la computación de niebla actúa como un intermediario entre la nube y los dispositivos finales, lo que acerca los servicios de procesamiento, almacenamiento y redes a los dispositivos finales. Estos dispositivos se llaman nodos de niebla. Se pueden implementar en cualquier lugar con una conexión de red. Cualquier dispositivo con conectividad informática, de almacenamiento y de red puede ser un nodo de niebla, como controladores industriales, conmutadores, enrutadores, servidores y cámaras de video vigilancia.

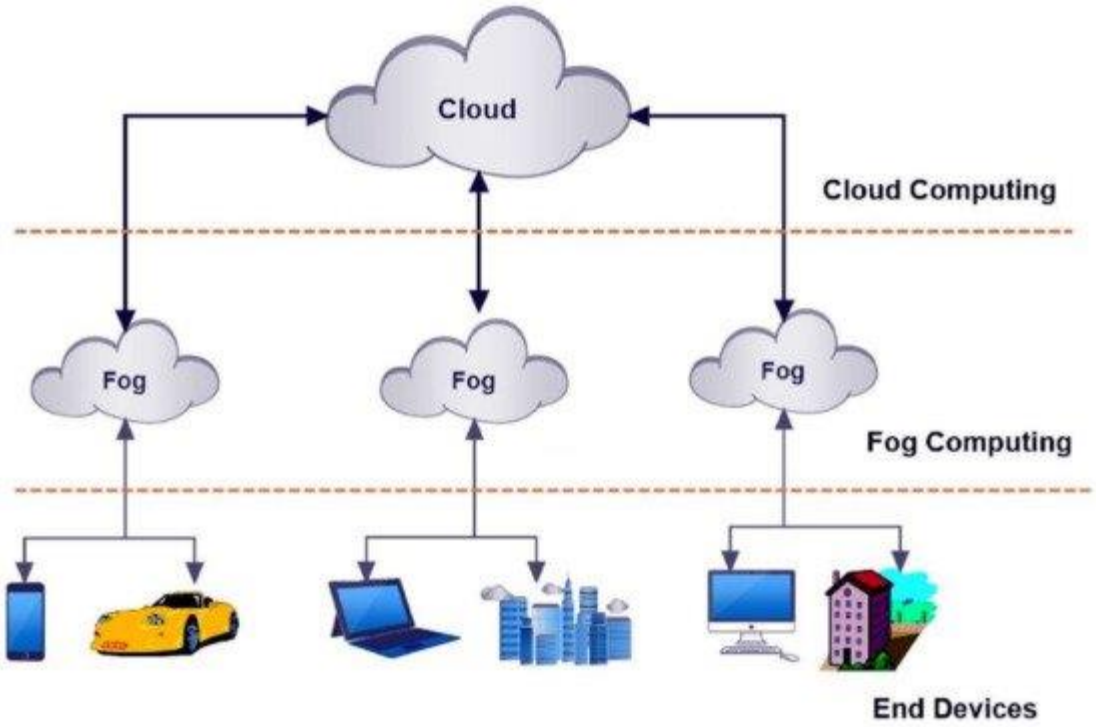

Figura 5 Modelo conceptual computación en la niebla.
(Fuente: https://iotahispano.com/2018/10/23/por-que-el-concepto-de-computos-de-outsourcing-de-iota-qubic-se-esta-convirtiendo-en-revolucionario/)

1.12.1 Beneficios de la computación de niebla

El cloud computing expande el modelo de cloud computing al borde de la red. Aunque la niebla y la nube utilizan recursos similares (redes, computación y almacenamiento) y comparten muchos de los mismos mecanismos y atributos (virtualización, multi-tenancy), la computación en niebla brinda muchos beneficios para los dispositivos IoT que se pueden resumir de la siguiente manera:

- ✓ Mayor agilidad empresarial: con el uso de las herramientas adecuadas, las aplicaciones de cómputo de niebla se pueden desarrollar e implementar rápidamente. Además, estas aplicaciones pueden programar la máquina para que funcione de acuerdo con las necesidades del cliente.

- ✓ Baja latencia: la niebla tiene la capacidad de soportar servicios en tiempo real (por ejemplo, juegos, transmisión de video).
- ✓ Distribución geográfica y a gran escala: la computación en niebla puede proporcionar recursos informáticos y de almacenamiento distribuidos para aplicaciones grandes y ampliamente distribuidas.
- ✓ Menor gasto operativo: Ahorro de ancho de banda de la red al procesar los datos seleccionados localmente en lugar de enviarlos a la nube para su análisis.
- ✓ Flexibilidad y heterogeneidad: la computación en niebla permite la colaboración de diferentes entornos físicos e infraestructuras entre múltiples servicios.
- ✓ Escalabilidad: la proximidad de la niebla de computación a los dispositivos finales permite escalar la cantidad de dispositivos y servicios conectados.

1.12.2 Arquitectura de la computación de niebla

La computación en niebla es un enfoque que lleva algunas de las operaciones de un centro de datos al borde de la red. La niebla proporciona servicios limitados de computación, almacenamiento y redes de manera distribuida entre los dispositivos finales y los centros de datos clásicos de computación en la nube. El objetivo principal de la computación de niebla es proporcionar una latencia baja y predecible para aplicaciones de IoT sensibles al tiempo.

Según los autores (Mukherjee M. , 2018) la arquitectura de cloud computing consta de seis capas: física y virtualización, monitoreo, preprocesamiento, almacenamiento temporal, seguridad y capa de transporte, como se muestra en la Figura 6, página 22.

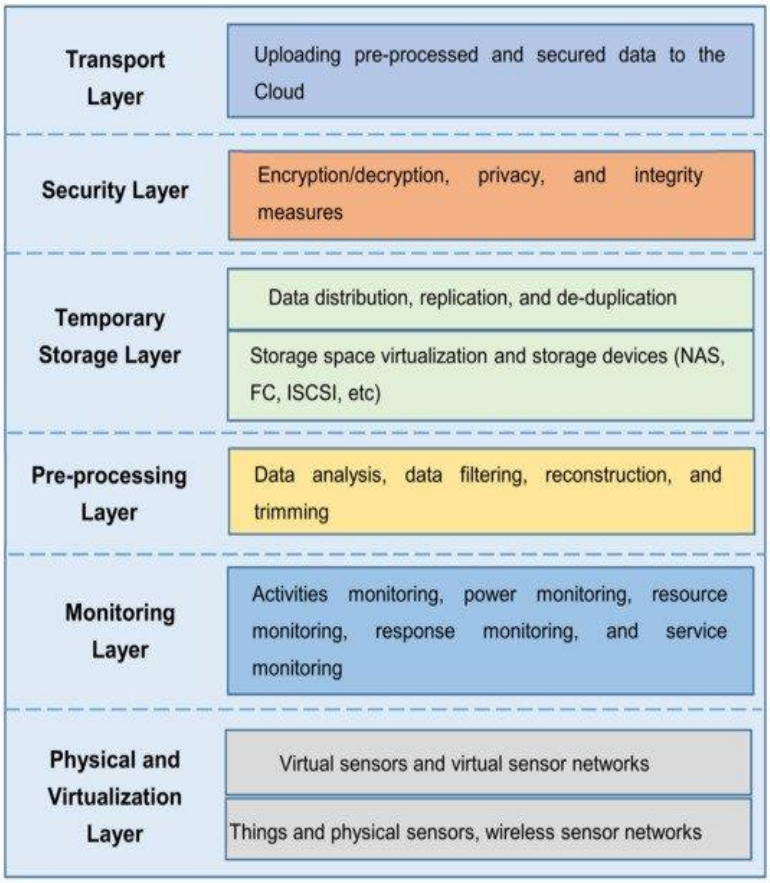

Figura 6 Arquitectura en capas de la computación de niebla.
(Fuente: https://iotahispano.com/2018/10/23/por-que-el-concepto-de-computos-de-outsourcing-de-iota-qubic-se-esta-convirtiendo-en-revolucionario/)

La capa física y de virtualización involucra diferentes tipos de nodos, como nodos físicos, nodos virtuales y redes de sensores virtuales. Estos nodos se gestionan y mantienen de acuerdo con sus tipos y demandas de servicio. Los diferentes tipos de sensores se distribuyen geográficamente para detectar el entorno y enviar los datos recopilados a las capas superiores a través de puertas de enlace para su posterior procesamiento y filtrado. Mientras que en la capa de monitoreo, se supervisa la utilización de recursos, la disponibilidad de sensores y nodos de niebla y elementos de red. Se supervisa el rendimiento y el estado de todas las aplicaciones y servicios implementados en la infraestructura. Además, se controla el consumo de energía de los nodos de

niebla; Dado que la informática de niebla utiliza muchos dispositivos con diferentes niveles de consumo de energía, las medidas de gestión de la energía pueden ser oportunas y efectivas.

La capa de preprocesamiento realiza tareas de gestión de datos. Los datos recopilados se analizan y el filtrado y el recorte de datos se llevan a cabo en esta capa para extraer información significativa. Los datos preprocesados se almacenan temporalmente en la capa de almacenamiento temporal. Cuando los datos se transmiten a la nube, ya no necesitan almacenarse localmente y pueden eliminarse del medio de almacenamiento temporal.

En la capa de seguridad, el cifrado / descifrado de datos entra en juego. Además, se pueden aplicar medidas de integridad a los datos para protegerlos de la manipulación. Finalmente, en la capa de transporte, los datos preprocesados se cargan en la nube para permitir que la nube extraiga y cree servicios más útiles. Para una utilización eficiente de la energía, solo una parte de los datos recopilados se carga en la nube. En otras palabras, el dispositivo de puerta de enlace que conecta el IoT a la nube procesa los datos antes de enviarlos a la nube. Este tipo de puerta de enlace se denomina puerta de enlace inteligente. Los datos recopilados de redes de sensores y dispositivos IoT se transfieren a través de puertas de enlace inteligentes a la nube. Los datos recibidos por la nube se almacenan y se utilizan para crear servicios para los usuarios. Basado en los recursos limitados de la niebla, un protocolo de comunicación para la computación de niebla debe ser eficiente, liviano y personalizable. Por lo tanto, elegir el protocolo de comunicación depende del escenario de aplicación de la niebla.

Artículos	Computación en la nube	Computación de niebla
Latencia	Alto	Bajo
Hardware	Almacenamiento escalable y potencia informática	Almacenamiento limitado y potencia informática
Ubicación de los nodos del servidor	Dentro de internet	En el límite de la red local.
Distancia entre cliente y servidor	Saltos múltiples	Un salto
Ambiente de trabajo	Interior	Al aire libre (p. Ej., Calles, jardines) o interior (p. Ej., Restaurantes)
Medidas de seguridad	Definido	Difícil de definir
Ataque a datos	Menos probabilidad	Probabilidad alta
Despliegue	Centralizado	Repartido
Conocimiento de ubicación	No	si

Tabla 2 Comparación entre computación en la nube y la niebla
(Fuente: Elaborada por el autor)

Para aumentar la eficiencia de las aplicaciones IoT, la mayoría de los datos generados por estos objetos / dispositivos IoT deben procesarse y analizarse en tiempo real (Atlam, Alassafi, Alenezi, Walters, & Wills, 2018). La computación en niebla llevará las capacidades de red, computación y almacenamiento en la nube al límite de la red, lo que abordará el problema en tiempo real de los dispositivos IoT y proporcionará aplicaciones de IoT seguras y eficientes (Ketel, 2017).

1.12.3 Desafíos de la niebla con el IoT

Aunque el paradigma de la computación de niebla ofrece muchos beneficios para diferentes aplicaciones de IoT, se enfrenta a muchos desafíos que se interponen en el camino de su implementación exitosa. Estos desafíos incluyen escalabilidad, complejidad, dinámica, heterogeneidad, latencia, energía y seguridad.

- ✓ Escalabilidad: la cantidad de dispositivos IoT es del orden de miles de millones, lo que genera una gran cantidad de datos y requiere una gran cantidad de recursos, como la potencia de procesamiento y el almacenamiento. Por lo tanto, los servidores de niebla

deberían poder admitir todos estos dispositivos con recursos adecuados. El verdadero desafío será la capacidad de responder al rápido crecimiento de los dispositivos y aplicaciones IoT (Choi, Kim, Lee, & Yi, Fog Operating System for User-Oriented IoT Services, 2017).

- ✓ Complejidad: dado que hay muchos dispositivos y sensores de IoT diseñados por diferentes fabricantes, elegir los componentes óptimos se está volviendo muy complicado, especialmente con diferentes configuraciones de software y hardware y requisitos personales. Además, en algunos casos, las aplicaciones con requisitos de alta seguridad requieren hardware y protocolos específicos para funcionar, lo que aumenta la dificultad de la operación (Luan, y otros, 2015).
- ✓ Dinámica: una de las características importantes de los dispositivos IoT es la capacidad de evolucionar y cambiar dinámicamente la composición de su flujo de trabajo. Este desafío alterará las propiedades internas y el rendimiento de los dispositivos IoT. Además, los dispositivos portátiles sufren el envejecimiento del software y el hardware, lo que provocará cambios en el comportamiento del flujo de trabajo y las propiedades del dispositivo. Por lo tanto, los nodos de niebla necesitarán una reconfiguración automática e inteligente de la estructura topológica y los recursos asignados (Luan, y otros, 2015).
- ✓ Heterogeneidad: hay muchos dispositivos y sensores de IoT diseñados por diferentes fabricantes. Estos dispositivos tienen varias capacidades en radios de comunicación, sensores, potencias informáticas, almacenamiento, etc. La gestión y coordinación de redes de dispositivos IoT tan heterogéneos y la selección de los recursos apropiados se convertirá en un gran desafío (Yi, Hao, Qin, & Li, 2015).

- ✓ Latencia: una de las principales razones para reemplazar la nube con cómputo de niebla es proporcionar baja latencia, especialmente para aplicaciones sensibles al tiempo. Sin embargo, hay muchos factores que presentan una alta latencia del rendimiento de la aplicación o el servicio en las plataformas de computación de niebla. La niebla con alta latencia conducirá a la insatisfacción del usuario (Choi, Kim, & Lee, 2017).
- ✓ Seguridad: aunque los nodos de niebla deberán protegerse mediante el uso de la misma política, controles y procedimientos y usar las mismas soluciones de seguridad física y ciberseguridad (Cisco, Fog Computing and the Internet of Things, 2018), el entorno de niebla en sí es vulnerable y menos seguro que la computación en la nube. Las medidas de seguridad y privacidad existentes de la computación en la nube no se pueden aplicar directamente a la niebla debido a su movilidad, heterogeneidad y geodistribución a gran escala (Mukherjee, y otros, 2017).
- ✓ Consumo de energía: el entorno de niebla implica una gran cantidad de dispositivos finales de niebla; el cálculo se distribuye y puede ser menos eficiente desde el punto de vista energético que el modelo centralizado de cómputo en la nube. Por lo tanto, reducir la energía consumida en la computación de niebla es un desafío importante que debe abordarse (Ni, Zhang, Lin, & Shen, 2017).

La computación en niebla es una nueva tecnología que necesita más investigación para superar los desafíos mencionados anteriormente, seleccionar la comunicación adecuada entre la niebla y la nube que garantice un alto rendimiento y una baja latencia de los nodos de niebla es un desafío que debe abordarse.

La preservación de la privacidad del usuario final es un problema importante que enfrenta la computación de niebla, los nodos de niebla están más cerca de los usuarios finales, lo que les permite recopilar datos más sensibles, incluidos registros financieros, identidad, uso de servicios públicos, ubicación y otros (Mukherjee, y otros, 2017). Además, como los nodos de niebla se distribuyen en grandes áreas, mantener un control centralizado es muy difícil. Proteger la privacidad de los nodos de niebla es un tema desafiante que requiere más investigación.

1.13 Edge Computing

Edge Computing permite la recopilación, procesamiento y tratamiento de datos en un dispositivo IoT, al borde de la red, es decir, sin necesidad de llevarlos a la nube. En este caso, se conectan los sensores a los controladores de automatización programables (PACs), reduciendo así los niveles de la comunicación dado que el PAC recibe, analiza y procesa la información recibida desde el dispositivo en el mismo punto de generación de los datos y sólo envía a la nube los datos que deben ser almacenados. Además de conseguir con este modelo una computación más eficiente, es posible habilitar el procesado, o pre procesado de los datos en la propia fuente de los mismos y se puede mantener un sistema total o parcialmente operativo aún en caso de que las comunicaciones de red hayan sido interrumpidas.

Este tipo de arquitectura resulta especialmente útil en escenarios en los que la latencia deba ser críticamente baja o en aquellos en los que el envío de todos los datos generados a un entorno cloud a través de la red no es práctica, posible o segura. Como ejemplos de estos entornos son la conducción autónoma o un entorno aislado con conectividad reducida como un dron.

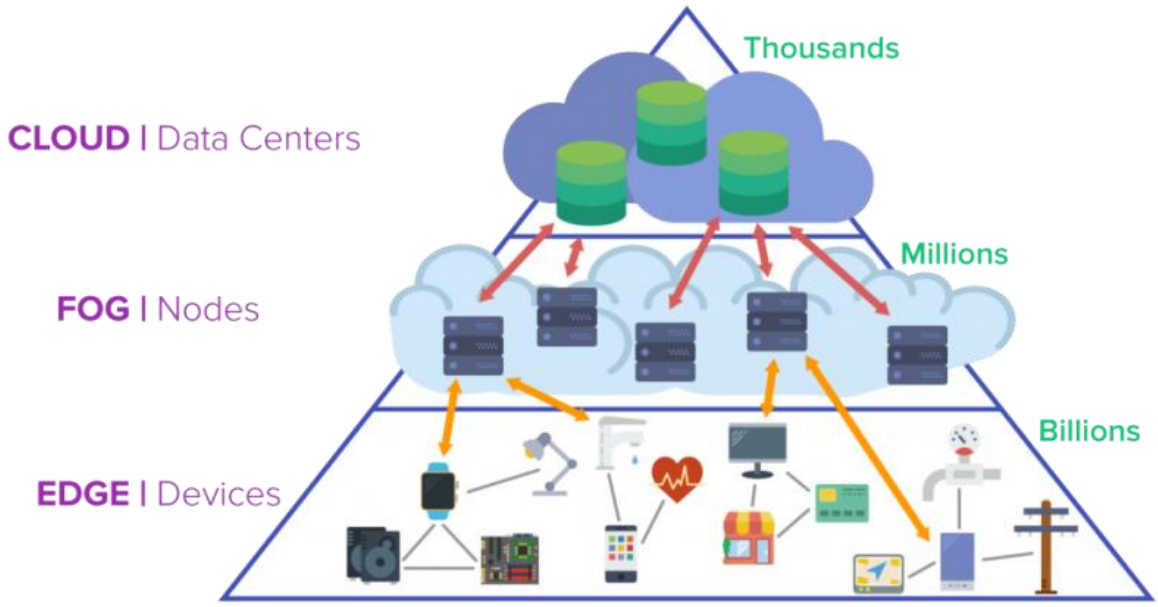

Figura 7 Modelo Cloud / Fog / Edge computing
(Fuente: https://erpinnews.com/fog-computing-vs-edge-computing)

1.14 Autenticación

Cada objeto en el IoT debe poder identificar y autenticar claramente otros objetos. Sin embargo, este proceso puede ser muy desafiante debido a la naturaleza del IoT; muchas entidades están involucradas (dispositivos, personas, servicios, proveedores de servicios y unidades de procesamiento) y otra cosa es que a veces los objetos pueden necesitar interactuar con otros por primera vez (objetos que no conocen). Debido a todo esto, se necesita un mecanismo para autenticar mutuamente las entidades en cada interacción en la IoT.

1.15 Protocolo 5G

Para realizar la implementación de IoT, IPv4 definitivamente se quedará corto para acomodar la gran cantidad de objetos identificables de IP. Esa es la razón por la que existe IPv6, que es

capaz de admitir 3. 4 × 1038 dispositivos. Sin embargo, tal número creará una gran cantidad de tráfico, lo que puede llevar a un mayor retraso y, por lo tanto, se necesita más ancho de banda.

La expectativa de la nueva generación de comunicación (5G) es proporcionar una velocidad entre 10-800Gbps, comparando este número con la tecnología actual (4G) con una velocidad de 2–1000 Mbps, 5G debe poder manejar el tráfico producido por los dispositivos IoT. También se espera que la tecnología 5G se adapte tanto a IPv4 como a IPv6; por tener traducción de framework IPv4 / lPv6. La implementación de 5G se definirá mediante muchas tecnologías actuales y en desarrollo, tales como: Redes heterogéneas (HetNets), Redes definidas por software (SDN), MIMO masivo y Acceso múltiple por radio, etc. Sin embargo, todas estas tecnologías vienen con sus propios desafíos de seguridad. Por ejemplo, HetNets tendrá un traspaso frecuente que afecta directamente el proceso de autenticación en la red, especialmente con el pequeño requisito de latencia de 5G. Además, la computación en la nube y las SDN aumentarán la cantidad de ataques DDoS debido a la característica de autoservicio bajo demanda de la computación en la nube. La seguridad de 5G y todas las tecnologías emergentes involucradas en 5G deben abordarse de manera extensa, a fin de garantizar la seguridad de IoT.

1.16 Consideraciones respecto de la seguridad IoT

El uso constante de dispositivos y aplicaciones de consumo en IoT traerá beneficios económicos y sociales a una gran población, estos procesarán una gran cantidad de datos sobre consumidores que hasta ahora no han sido de fácil acceso para las organizaciones, sin embargo, la recopilación de cantidades masivas de datos personales y complejidades tecnológicas es un motivo de preocupación relacionado con la privacidad y la seguridad. Por lo tanto, los

beneficios solo se lograrán si los dispositivos pueden diseñarse con la confianza de los consumidores a través de políticas bien estructuradas de las organizaciones.

Las oportunidades presentadas por el IoT vienen con vulnerabilidades que generan inquietudes sobre la privacidad y seguridad de los datos, y algunos de estos temores pueden abordarse, mientras que otros solo pueden restringirse para minimizar el impacto. Algunos se opondrán a la idea de restricciones relacionadas con la privacidad y la seguridad argumentando que el beneficio económico de usar los datos específicos es adaptar las decisiones económicas y que esto supera cualquier costo social. A medida que las organizaciones continúan encontrando formas de obtener ganancias del IoT, presionarán para obtener más poder para resistir más restricciones. Los datos generados por la IoT y la capacidad de revelar información personal sobre las actividades humanas diarias serán un elemento crucial del análisis de Big Data que busca descubrir tendencias y patrones ocultos.

Los consumidores de IoT esperan que la información personal sea segura y no se comparta, y se preservará y procesará de manera segura para evitar la intrusión de usuarios no autorizados. Sin embargo, también se dan cuenta de que proporcionar más datos personales será beneficioso para el uso de los servicios de IoT provistos. Los consumidores dependen de estos dispositivos para hacerles la vida más fácil y alcanzar sus metas, por lo que brindan información que alimenta el uso de las herramientas. Cuando el consumidor no recibe ningún aviso sobre los datos que se recopilan y quién más los recibe, es difícil formular expectativas sobre cómo se pueden usar los datos. Es posible que los consumidores no comprendan el alcance de los datos recopilados y el

impacto futuro que esto podría tener en su privacidad. Este impacto futuro es lo que debe protegerse antes de que el problema sea generalizado e inmanejable.

En un entorno IoT, se pueden generar diferentes tipos de paquetes y tráfico variable desde numerosos dispositivos, incluidos sensores. En consecuencia, el tema de controlar de forma proactiva dicha información en el entorno de red existente se está volviendo progresivo. Además, en lo que respecta a la seguridad, como un entorno de IoT tiene limitaciones de rendimiento, ya que se compone de dispositivos sensores con especificaciones inferiores, existe el problema de que las tecnologías de seguridad de los dispositivos existentes son difíciles de aplicar (Agarwal, 2014). Sin embargo, si no se toman las medidas de seguridad adecuadas, existen riesgos de fuga de información, falsificación de datos y ataques de denegación de servicio a gran escala.

Capitulo II: Estado del arte

El rápido crecimiento de IoT ha provocado una enorme atención por parte de la comunidad de investigación. Para resaltar los últimos hallazgos y las direcciones de investigación en un campo tan cambiante, se presentaron una gran cantidad de encuestas para arrojar luz sobre las tendencias y desafíos recientes de IoT, como (i) protocolos y tecnologías habilitadoras, (ii) dominios de aplicación, (iii) conciencia del contexto, (iv) marcos legales, (v) ataques contra IoT, (vi) modelos de acceso, (vii) protocolos de seguridad y (viii) técnicas de detección de intrusos.

En esta sección se examinan algunos estudios relacionados que han analizado ampliamente los sistemas de IoT, y también abordan desafíos de seguridad relevantes.

Identificación	Objetivo general	Categorías / Variables	Instrumentos recolección de la información	Resultado
Rolf H. Weber, "Internet of things: Privacy issues revisited" in University of Zurich Switzerland computer law & security review, 2015.	Elaborar un análisis exhaustivo de los protocolos y mecanismos de seguridad disponibles para proteger las comunicaciones en el IoT.	Seguridad IoT Estándar IEEE 802.15.4 Protocolos Seguridad extremo a extremo Agujeros de seguridad	Estudio bibliográfico apoyado en la revista internacional y archivo Ad Hoc Netwoks, articulos de la Revista internacional de comunicación y redes de futuras generaciones, y articulos de IEEE Explore.	Concluye el autor que en IoT es todo un desafío la privacidad y seguridad. IoT debe afrontar el desafío de recopilar una enorme cantidad de datos y mantener su seguridad y privacidad. Propuso desarrollar tecnologías sólidas que se ocupen de la seguridad en la comunicación y el almacenamiento de los datos, como es el caso de los datos relacionados con la salud, información financiera o algunos datos críticos de defensa o datos confidenciales similares.
I. Andrea, C. Chrysostomou, G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges", 2015 IEEE Symposium on Computers and Communication (ISCC), 2015.	Analizar las diferentes vulnerabilidades y posibles ataques en el IoT.	Seguridad Protocolos Privacidad de los datos	Estudio bibliográfico apoyado en fuentes de artículos indexados y conferencias de tecnología, artículos de IEEE Xplore y Computer Science and Electronics Engineering, Apoyo en fabricantes de tecnología como Cisco Systems Inc.	Clasificaron los ataques de las diferentes capas del modelo IoT en cuatro grupos según la vulnerabilidad utilizada por un adversario en el ataque.

Identificación	Objetivo general	Categorías / Variables	Instrumentos recolección de la información	Resultado
S. W. Heo, H. W. Kim, "An Analysis of IoT Security Requirements And oneM2M Security Technology", Communications of the Korean Institute of Information Scientists and Engineers, 2017.	Analizar el servicio de seguridad proporcionado por la capa de seguridad.	Análisis Seguridad IoT Plataforma Vulnerabilidades	Estudio bibliográfico apoyado en fuentes de artículos indexados y conferencias de tecnología en IEEE Xplore.	Analizaron la estructura de seguridad oneM2M donde ilustran los autores la arquitectura de oneM2M, concluyendo que ésta consta de tres capas: Seguridad, Abstracción y Entorno. Se centraron en analizar el servicio de entorno seguro proporcionado por la capa Seguridad.
Nam Ky Giang, Rodger Lea, "Fog at the Edge: Experiences Building an Edge Computing Platform", IEEE International Conference on Edge Computing (EDGE), 2018.	Proponer un modelo de programación de alto nivel que permita a los desarrolladores especificar cómo se puede implementar la aplicación en muchos dispositivos informáticos de niebla .	Cloud computing Edge computing Red perimetral Nube	Estudio bibliográfico apoyado en fuentes de artículos indexados y conferencias de tecnología, artículos de IEEE Xplore y ACM Computing Surveys.	Este trabajo demostró que el modelo de aplicación en sí mismo debe ser consciente de la plataforma informática subyacente en la que se ejecuta la aplicación. En el lado negativo, el modelo propuesto no divide explícitamente la aplicación en subcomponentes, lo que hace imposible tener diferentes estrategias de implementación sin cambiar la lógica de la aplicación.
Lopez Miguel A,Muñoz F.Isabel, "SAT-IoT: An Architectural Model for a High-Performance Fog/Edge/Cloud IoT Platform", Sistemas Avanzados de Tecnología, S.A., Technical University of Madrid, 2019	Proponer un modelo de referencia arquitectónico extendido completo que se está utilizando como base de diseño e implementación de una nueva plataforma IoT (llamada SAT-IoT).	Plataforma IoT Edge Fog Redes híbridas Implementación	Estudio bibliográfico apoyado en fuentes de artículos indexados y conferencias de tecnología, artículos de IEEE Xplore, libros como Tecnologías informáticas de borde para Internet de las cosas: un manual y Una arquitectura de referencia para Internet de las cosas.	Definieron un nuevo modelo arquitectónico que incluye arquitectura Fog / Edge y cubre otras demandas de IoT, como los servicios de protección de seguridad basados en Blockchain.

Si bien las destacadas contribuciones de investigación mencionadas anteriormente abordaron específicamente los temas de las arquitecturas de IoT y las tecnologías correspondientes, es necesario profundizar en aspectos de seguridad que aborden los riesgos en cada una de las capas IoT de manera separada por cuanto con una solución unificada no sería insuficiente para proteger un sistema Iot.

Capítulo III: Planteamiento del problema

Con todos los beneficios que IoT puede proporcionar también surgen nuevos desafíos de seguridad y privacidad en términos de la autenticidad de la confidencialidad y la integridad de los datos detectados, recopilados e intercambiados por los objetos de IoT, junto con la autorización y el no repudio que también deben considerarse. Los datos y la información generada deben ser seguros a lo largo de su ciclo de vida. Estos desafíos hacen que las implementaciones de IoT sean extremadamente vulnerables a diferentes tipos de ataques de seguridad, lo que resulta en entornos de IoT inseguros.

3.1 Ciberseguridad

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ataques cibernéticos generalmente tienen como objetivo acceder, cambiar o destruir información; extorsionar a los usuarios o interrumpir procesos comerciales. La ciberseguridad no solo protege la confidencialidad y la privacidad, sino también la disponibilidad y la integridad de los datos.

La implementación de medidas efectivas de ciberseguridad es particularmente desafiante hoy dado que existen más dispositivos que personas, y los atacantes se están volviendo más innovadores. Para el caso de América Latina y según informe de (Kaspersky, 2018) en el 2018 se registró un alza de 60% en ataques cibernéticos, más de 746 mil ataques de malware diarios, lo que significa un promedio de 9 ataques de malware por segundo.

De otra parte, un reciente estudio de la Corporación finlandesa de seguridad cibernética y privacidad (F-Secure, 2017), identificó dieciocho vulnerabilidades en dos cámaras IP hechas por el fabricante chino Foscam, entre las que se encuentran: no hacer las contraseñas predeterminadas al azar, no bloquear a los usuarios que intentan demasiadas contraseñas incorrectas, no restringir el acceso a los archivos y directorios críticos, además de capacidades que no deberían estar presentes, como el acceso oculto a Telnet o las credenciales codificadas que permiten mediante un ataque omitir incluso la contraseña única de un usuario. Si se explotan esas múltiples vulnerabilidades, un atacante podría tomar el control de la cámara y hacerla funcionar tal y como un usuario legítimo pueda hacerlo. Las webcams pueden ser hackeadas y no es solo una webcam, también es un servidor y ese servidor es vulnerable. Si los atacantes pueden acceder incluso al dispositivo más pequeño de una red ahora tendrá un trampolín para acceder a los demás recursos y por tanto es necesario garantizar que los accesos a la misma sean legítimos. Hasta este punto ya existe algo de preocupación, pero más grave aún es el hecho que hay millones de estas cámaras instaladas alrededor del mundo y aunque parezca irónico lo que se supone proporciona una medida de seguridad también podría hacer un sistema más vulnerable.

La seguridad de la información es un aspecto que no debe tomarse a la ligera, ejemplo de ello sucedió en mayo de 2017 con un ataque masivo de ransomware denominado Filecoder.WannaCryptor.D (Eset, 2017), que resultó una ser una versión mejorada de WannaCry (Avast, 2018), afectó a empresas y particulares de todo el mundo incluyendo grandes corporaciones y organismos públicos, impactando principalmente hospitales del Servicio Nacional de Salud Británico, al sistema bancario de Rusia, al servicio de ferrocarriles de

Alemania, las compañía multinacionales Fedex, Renault y Telefónica de España, así como a universidades en Grecia e Italia (MINSAP, 2017), prueba de ello y como recordatorio para todos del por qué vale la pena tomar las precauciones necesarias.

3.2 Iot y Ciberseguridad

En IoT se integran automóviles, productos de consumo, productos para el hogar, rastreadores de mascotas, televisores inteligentes, etc., hay un futuro prometedor con los dispositivos IoT, futuro que ya está aquí, los dispositivos inteligentes están en todos lados para hacer más eficientes las vidas y negocios de sus usuarios. Sin embargo, dado que estos dispositivos almacenan datos personales y se comunican con otros dispositivos conectados a Internet, se hace necesario proteger la privacidad de los datos.

Los dispositivos IoT recopilan datos durante su uso y comparten esa información con sus fabricantes sin que los usuarios lo sepan. En agosto de 2014, Hewlett Packard Enterprise Security (HP, 2014) publicó un estudio que detalla las preocupaciones de seguridad más comunes para los usuarios que utilizan dispositivos IoT, el cual revela que el 70 por ciento de los dispositivos y aplicaciones de IoT más utilizados son vulnerables a ataques de seguridad en contraseñas, el cifrado y la falta de permisos de acceso de los usuarios.

Según el informe, HPE utilizó la solución HP Fortify on Demand, una herramienta utilizada para pruebas de seguridad de aplicaciones para probar los sistemas IoT y que combinan pruebas de seguridad manuales y el uso de herramientas automatizadas, para explorar los diez dispositivos más populares, descubriendo que el 80% de ellos tienen fallos en la autenticación y

6 de cada 10 dispositivos con interfaz de usuario son vulnerables. Los dispositivos probados, junto con sus aplicaciones móviles y componentes en la nube, eran de fabricantes de televisores, cámaras web, termostatos, tomas de corriente remotos, controladores de riego, centros de control de múltiples dispositivos, cerraduras de puertas, alarmas domésticas y puertas de garaje. Esas advertencias de seguridad evidenciaron fallos en la privacidad, debido a la recopilación de información personal; autorizaciones insuficientes, el 80% de los dispositivos no requieren contraseñas complejas, y muchos permiten contraseñas de la forma 1234; falta de cifrado en la transmisión de los datos entre la nube y la red local en el 70% de los dispositivos IoT; interfaz web inseguro, XSS persistente, pobre gestión de sesiones, credenciales predeterminadas débiles y transmitidas en texto plano; y finalmente protección inadecuada del software, pues el 60% no usa cifrado cuando descarga actualizaciones.

Estos datos no son muy tranquilizadores, por cuanto la evolución de los IoT es desarrollada sobre la funcionalidad y tecnología, debido a la función restringida, la mayoría de los dispositivos de IoT no implementan las defensas necesarias para el sistema y la red; por ejemplo, los dispositivos IoT ligeros (sin muchas capacidades de procesamiento y con anchos de banda limitados) no tienen la unidad de administración de memoria (MMU), por lo que el aislamiento de la memoria, la aleatorización del diseño del espacio de direcciones y otras medidas de seguridad de la memoria no se pueden aplicar a estos dispositivos. Algoritmos de encriptación y autenticación como la criptografía asimétrica, no deben implementarse en tales dispositivos por cuanto ocupan demasiados recursos informáticos y causan un gran retraso que afecta gravemente el funcionamiento normal y reduce el rendimiento para ese tipo de dispositivos IoT. En consecuencia, es fácil para los atacantes utilizar vulnerabilidades de memoria para comprometer

estos dispositivos. Además, muchos dispositivos IoT incluso se comunican con el servidor sin ningún tipo de cifrado o utilizan el cifrado SSL sin verificar el certificado del servidor.

Según el Proyecto de Internet de las cosas (IoT) de OWASP, las áreas de ataque de IoT son las siguientes:

- ✓ Interfaz web insegura
- ✓ Autenticación / autorización insuficiente
- ✓ Servicios de red inseguros
- ✓ Falta de cifrado de transporte
- ✓ Preocupaciones sobre la privacidad
- ✓ Interfaz de nube insegura
- ✓ Interfaz móvil insegura
- ✓ Configuración de seguridad insuficiente
- ✓ Software / Firmware inseguro
- ✓ Pobre seguridad física

Se requerirán tecnologías de seguridad para proteger los dispositivos y plataformas de IoT tanto de ataques de información como de manipulación física, para cifrar sus comunicaciones y enfrentar nuevos desafíos. Los estándares y protocolos utilizados actualmente no pueden manejar gran cantidad de tráfico de dispositivos inteligentes o móviles que se conectan a Internet al mismo tiempo, para cumplir con los requisitos actuales de IoT (bajo consumo de energía, algoritmos optimizados, etc.), es necesaria una arquitectura bien definida que admita una gran cantidad de dispositivos para establecer un marco de seguridad para la configuración de un entorno IoT eficiente de estos dispositivos y una seguridad mejorada.

Para cada ataque dirigido a alguna de las capas IoT hay al menos una posible solución. Si se implementan de manera separada todas estas soluciones en IoT, se generarán muchos gastos generales y se reducirá su rendimiento. Los estándares y protocolos utilizados actualmente no pueden manejar gran cantidad de tráfico de dispositivos inteligentes o móviles que se conectan a Internet al mismo tiempo. Para cumplir con los requisitos actuales de IoT (bajo consumo de energía, algoritmos optimizados, etc.), es necesario una arquitectura bien definida que admita una gran cantidad de dispositivos.

Una solución a los problemas planteados y que permita resolver las situaciones de seguridad y privacidad de los datos, surge como propuesta elaborar un modelo para diseñar arquitectura de red que sea efectiva y más segura; que contemple todas las capas de la arquitectura de IoT dado que cada dominio IoT tiene diferentes riesgos de seguridad y, por lo tanto, utiliza diferentes tecnologías para la seguridad.

Capitulo IV: Justificación

Como IoT usa una arquitectura de red que es similar a la arquitectura de red tradicional para la comunicación entre diferentes dispositivos, también se heredan fallas de la arquitectura de red tradicional. Con el desarrollo de IoT, también se han inventado muchos tipos de ataques para violar la seguridad de los dispositivos IoT. Los investigadores han propuesto diferentes soluciones para atacar estos ataques, sin embargo, la implementación de todas estas medidas y técnicas de seguridad en conjunto consume la computación y la energía de la batería de los dispositivos, lo cual no es aceptable para la tecnología IoT y sus dispositivos. Existe la necesidad de un mecanismo de seguridad que maneje los problemas de máxima seguridad, pero debe ser liviano y robusto para adaptarse a la tecnología IoT.

En el punto de seguridad del sistema, debido a la diversidad de dispositivos IoT, es difícil diseñar una defensa de sistema común para los dispositivos heterogéneos, especialmente en el área de la industria. Por lo tanto, la forma de descubrir y lidiar con tantas vulnerabilidades de seguridad entre los distintos dispositivos de IoT debe abordarse con urgencia.

Recientemente, hay cada vez más estudios centrados en la protección de la privacidad de los datos de IoT. Muchas soluciones utilizan el enmascaramiento y el cifrado de datos, como el algoritmo homomórfico, para proteger la información confidencial, pero estas soluciones reducen la disponibilidad de los datos originales y aumentan la demora en el procesamiento de los datos. El método de protección de la privacidad efectiva también debe seguir siendo una alta disponibilidad de datos originales y minimizar el retraso al mismo tiempo. Otro problema importante entre los métodos actuales de protección de la privacidad es el ámbito de aplicación

limitado. La mayoría de los métodos solo se aplican a los escenarios de aplicación específicos como red inteligente, medicina inteligente, redes de automóviles o intercambio de datos de privacidad con el servicio en la nube. Las medidas de protección más completas para los datos privados de IoT requieren una investigación más profunda.

Los desafíos de seguridad de IoT se pueden dividir en dos clases; Retos tecnológicos y Retos de seguridad. Como se describió anteriormente, los desafíos tecnológicos surgen debido a la naturaleza heterogénea y ubicua de los dispositivos de IoT, mientras que los desafíos de seguridad están relacionados con los principios y funcionalidades que deben aplicarse para lograr una red segura. Los desafíos tecnológicos suelen estar relacionados con las tecnologías inalámbricas, la escalabilidad, la energía y la naturaleza distribuida, mientras que los desafíos de seguridad requieren la capacidad de garantizar la seguridad mediante la autenticación, la confidencialidad, la seguridad de extremo a extremo, la integridad, etc. La seguridad debe cumplirse en IoT durante todo el desarrollo y el ciclo de vida operativo de todos los dispositivos y hubs de IoT.

El marco de IoT es susceptible de ataques en cada capa; Por lo tanto, hay muchos desafíos y requisitos de seguridad que deben abordarse. El estado actual de la investigación en IoT se centra principalmente en los protocolos de autenticación y control de acceso, pero con el rápido avance de la tecnología es esencial incorporar nuevos protocolos de red como IPv6 y 5G.

El IoT tiene un gran potencial para transformar la forma en que vivimos hoy. Pero, la principal preocupación en la realización de marcos completamente inteligentes es la seguridad.

Si las cuestiones de seguridad como la privacidad, la confidencialidad, la autenticación, el control de acceso, la seguridad de extremo a extremo, la gestión de confianza, las políticas y estándares globales se abordan por completo, es posible presenciar la transformación de todo por parte de IoT en un futuro próximo.

Dentro del contexto planteado, se nos genera la suficiente motivación en la presente investigación para hacer frente a un problema actual de la vida real y no menos importante, la seguridad de la información que se genera IoT. En cuanto a la seguridad y privacidad de los datos que se producen en entornos IoT existen variadas propuestas y modelos para abordar la complejidad del problema que conlleva asegurar esos datos de un entorno heterogéneo y con recursos de hardware limitados; infortunadamente esas propuestas no plantean un modelo que albergue el aseguramiento IoT de una manera global, los estudios plantean la viabilidad de fortalecer el sistema IoT en alguna de las tres capas de su arquitectura, es por ello que se pretende abordar el problema presentando una solución que contribuya a la generación de un modelo seguro y eficiente desarrollado sobre las tres capas IoT, Percepción, Red y Aplicación.

Capítulo V: Objetivos

5.1 Objetivo general

Proponer un modelo de ciberseguridad con enfoque en la confiabilidad, privacidad y seguridad de los datos enmarcado dentro de las tres capas de la arquitectura IoT y conectividad 5g.

5.2 Objetivos específicos

- Identificar las principales vulnerabilidades de seguridad conocidas que se presentan en cada una de las capas arquitectónicas de IoT: Percepción, Red y Aplicación.
- Describir un marco conceptual donde se ilustren los requisitos mínimos de un modelo de confianza exitoso para el entorno de IoT.
- Analizar las características, ventajas, tendencias y vulnerabilidades de los nuevos algoritmos de criptografía simétricos ligeros propuestos para IoT.
- Analizar las características y tendencias entre 5G y su implementación para IoT.
- Proponer un modelo de ciberseguridad que proteja cada una de las capas arquitectónicas de IoT.

Capítulo VI: Metodología

6.1 Tipo de investigación

El tipo de investigación asociado a este trabajo es la exploratoria por lo que permite examinar un tema con muchas dudas respecto de su implementación y nos ayudará a familiarizarnos con aspectos de seguridad aún no implementados en entornos IoT.

6.2 Diseño de investigación

El diseño de la investigación se desarrollará sobre la base de los siguientes apectos.

1. Formulación y planteamiento del problema.
2. Revisión bibliográfica y documental.
3. Redacción de los objetivos: general y específicos.
4. Selección de las fuentes de información.
5. Análisis de la información recolectada a través de las investigaciones documentales.
6. Determinar niveles de seguridad en las diferentes capas
7. desarrollar esquemas para diseñar un modelo con niveles de seguridad aceptables y determinar los beneficios del proyecto.
8. Elaboración de recomendaciones y conclusiones.
9. Presentación del informe de investigación.

6.3 Métodos de investigación

El método utilizado en la investigación de este trabajo será descriptivo.

6.4 Técnicas e instrumentos de recolección de datos

Para la obtención de la información necesaria en la presente investigación se realizaron consultas y técnicas de:

- ✓ Artículos de bases de datos académicas
- ✓ Investigación Bibliográfica.
- ✓ Investigación en Internet.
- ✓ Análisis.

6.5 Bases de datos académicas consultadas

- ✓ Google Scholar
- ✓ Scopus
- ✓ Science Direct
- ✓ IEEE Xplore

6.6 Plan recolección de la información

Para la recolección de información se llevó a cabo una exhaustiva búsqueda de recursos bibliográficos (revistas, libros, artículos) de internet, además de la observación de videos sobre debates sobre temas de seguridad del IoT.

Se consideraron también entrevistas realizadas por algunos medios internacionales a profesionales de otros países que están directamente relacionados e investigando esta tendencia.

6.7 Plan de procesamiento y análisis de la información

Se realizó un análisis de la información relevante en la adopción del IoT y los niveles de seguridad que se están considerando, con el fin de poder desarrollar la propuesta de la mejor manera posible. Para ello se consideró realizar lo siguiente:

- ✓ Recolección de información
- ✓ Registrar las fuentes de información
- ✓ Procesamiento de la información recabada.
- ✓ Plasmar los esquemas propuestos.
- ✓ Establecer las conclusiones y recomendaciones.

6.8 Recursos

Para el desarrollo de la presente investigación se requirió una computadora con procesador Intel Core I5 con memoria Ram de 8 GB, además de acceso a Internet; así como las respectivas credenciales de acceso a las bases de datos académicas descritas anteriormente.

6.9 Hipótesis

¿Es posible desarrollar un modelo de ciberseguridad con enfoque en la confiabilidad, privacidad y seguridad de los datos enmarcado dentro de las tres capas de la arquitectura IoT y conectividad 5g?

6.10 Producto esperado

Teniendo en cuenta los objetivos planteados en el anteproyecto, se pretende entregar como resultado:

- ✓ Documento de tesis
- ✓ Artículo publicado en revista indexada
- ✓ Ponencia orientada a la implementación de ciberseguridad para sistemas IoT en redes 5G.

Capítulo VII: Vulnerabilidades de IoT

En el punto de seguridad del sistema, debido a la diversidad de dispositivos IoT, es difícil diseñar una defensa de sistema común para los dispositivos heterogéneos, especialmente en el área de la industria. Por lo tanto, la forma de descubrir y lidiar con tantas vulnerabilidades de seguridad entre los distintos dispositivos de IoT debe abordarse con urgencia.

Autores como Kaur Damandeep, P. Singh, D. Singh, G. Tripathi y A.J. Jara explican diferentes vulnerabilidades y posibles ataques a IoT, es así como los autores (Hadjichristofi, 2015) clasifican los ataques en cuatro grupos según la vulnerabilidad utilizada por un adversario en el ataque. En (Singh, 2014) y (Damon, 2003) se describen posibles ataques en la capa OSI. (Jara, 2014), (Liu, 2012) y (Mazhar, 2015) se centran en los desafíos de seguridad de un sistema de IoT; sin embargo, la mayoría de estos autores abordan solo tipos específicos de amenazas basadas en objetivos de seguridad específicos, no hay técnicas propuestas tan sólidas que resuelvan la mayoría de los problemas de seguridad de IoT.

Además, (A. Mosenia, 2017) utilizaron el modelo de referencia de siete niveles de Cisco para presentar varios escenarios de ataque correspondientes. Los autores exploraron numerosos ataques dirigidos a IoT y señalaron sus posibles enfoques de mitigación. Los autores destacaron la importancia de poseer un enfoque proactivo para asegurar el entorno de IoT.

En un trabajo alternativo, (FA Alaba, 2017) analizaron la seguridad de IoT al revisar las soluciones de seguridad existentes y proponer una taxonomía de las amenazas y vulnerabilidades actuales en el contexto de varios entornos de implementación de IoT. En particular, la taxonomía

distinguió entre cuatro clases, que incluyen, aplicación, arquitectura, comunicación y datos. Los autores examinaron varias amenazas y las discutieron para cada dominio de implementación. Además, se discutieron varios desafíos de IoT, que actualmente enfrenta la comunidad investigadora. En este contexto, los autores argumentaron que la heterogeneidad de los dispositivos IoT junto con sus limitaciones de recursos definen un problema grave, que dificulta la escalabilidad de las posibles soluciones de seguridad.

Los ataques que puede sufrir IoT se dividen en cuatro categorías básicas, ataque físico, ataque a la red, ataque de software y ataque de cifrado, como se ilustra en la tabla 1, página 13.

<table>
<tr><th>ATAQUE FÍSICO</th><th>ATAQUE DE RED</th><th>ATAQUE DE SOFTWARE</th><th>ATAQUE DE CIFRADO</th></tr>
<tr><td>Manipulación de nodo</td><td>Análisis de tráfico</td><td>Virus</td><td>Canal lateral</td></tr>
<tr><td>Interferencia RFID</td><td>RFID Spoofing</td><td rowspan="2">Spyware, Nodo malicioso</td><td>Hombre en medio</td></tr>
<tr><td>Nodo atascado</td><td>Clonación RFID</td><td rowspan="5">Criptoanálisis</td></tr>
<tr><td>Inyección de nodo malicioso</td><td>Ataque de sumidero</td><td>Troyanos</td></tr>
<tr><td>Daño físico</td><td>Ataque de sybil</td><td>Scripts malicioso</td></tr>
<tr><td>Ingeniería social</td><td>DDoS</td><td rowspan="3">DoS</td></tr>
<tr><td>Ataque privación de sueño</td><td rowspan="2">Hombre en medio</td></tr>
<tr><td>Inyección de código malicioso</td></tr>
</table>

Tabla 3 Clasificación de ataques más significativos IoT
(Fuente: Elaborada por el autor)

A continuación, se presenta una lista creciente de amenazas con una breve descripción. Estas amenazas son específicamente capaces de evitar o intentar eludir la privacidad y seguridad de los datos y/o comunicaciones a través de medios tales como obtener acceso ilegítimo a nodos individuales / etiquetas RFID o a la red en su totalidad.

7.1 Ataques Físicos

Los dispositivos perimetrales operan en entornos hostiles en los que es posible el acceso físico a los dispositivos, lo que los hace muy vulnerables a los ataques de hardware / software. El atacante, con acceso físico al dispositivo, puede extraer información criptográfica valiosa, alterar el circuito, modificar la programación o cambiar el sistema operativo. Los ataques físicos contra los nodos del borde pueden causar destrucción permanente. Por lo tanto, su objetivo principal es extraer información para uso futuro, por ejemplo, encontrar la clave compartida fija. Un ataque reciente tan conocido fue el termostato Nest (Hernandez, 2104), en el que el atacante intenta reemplazar el firmware predeterminado por uno malicioso. Este ataque permite al atacante controlar el termostato, incluso cuando ya no tiene acceso físico al dispositivo.

- ✓ Interferencia de RF en RFIDs, consiste en realizar un ataque DoS enviando señales de ruido sobre las señales de radiofrecuencia. Con este ataque, los canales de RF están atascados de tal manera que los lectores de etiquetas no pueden leerlas y como resultado los servicios previstos basados en las etiquetas RFID dejan de estar disponibles. Por ejemplo, un atacante puede bloquear todo un edificio bloqueando todas las puertas basadas en RFID.
- ✓ Manipulación del dispositivo, o nodo alterado para obtener información confidencial o la clave de cifrado.
- ✓ Nodo atascado en WSNs, consiste en realizar un ataque DoS perturbando la señal inalámbrica.
- ✓ Inyección de Nodo Malicioso, se da cuando un atacante adiciona un nuevo nodo malicioso a la red luego de reemplazar un nodo legitimo al que le fue extraída la

información luego de obtener control del mismo. Una vez adicionado el nodo malicioso se procede a inyectar un segundo nodo malicioso el cual se sincronizará con el primer nodo malicioso para que trabajen coordinados y lograr el ataque deseado. Ambos nodos maliciosos inician el ataque enviando mensajes a un nodo atacado con la intención de crearle una colisión de datos.

- ✓ Inyección de código malicioso, el adversario introduce físicamente un código malicioso en el nodo del sistema IoT, es posible obtener el control total del sistema IoT.

El ataque de inyección de nodo malicioso ha sido el ataque peligroso ya que no solo se están parando los servicios, sino que también se modifican los datos.

7.2 Ataques de Red

Se dan en la segunda capa de la arquitectura IoT.

- ✓ Ataque de análisis de tráfico, cuando un atacante intercepta las comunicaciones del sistema IoT obteniendo información de la red.
- ✓ RFID Spoofing, un adversario falsifica señales RFID. Luego captura la información que se transmite desde una etiqueta RFID. Los ataques de suplantación consisten en entregar información incorrecta que parece ser correcta y que el sistema acepta.
- ✓ Clonación por RFID, En este ataque, el adversario copia datos de una etiqueta RFID preexistente a otra etiqueta RFID. No copia el ID original de la etiqueta RFID. El atacante puede insertar datos incorrectos o controlar los datos que pasan a través del nodo clonado.

- ✓ Ataque de sumidero, un adversario compromete un nodo dentro de la red y realiza el ataque utilizando este nodo. El nodo comprometido envía la información de enrutamiento falsa a sus nodos vecinos en el sentido de que tiene la ruta de distancia mínima a la estación base y luego atrae el tráfico. A continuación, puede alterar los datos y también eliminar los paquetes.
- ✓ Ataque de sybil, un nodo malicioso toma las identidades de múltiples nodos y actúa como ellos. Los nodos falsificados pueden ser un dispositivo existente en la red WLAN o un dispositivo de ataque virtual. Cada nodo falso puede usarse como intermediario para robar información privada de clientes reales, y cuando una gran cantidad de nodos falsificados acceden a las redes y envían grandes cantidades de datos, esto bloqueará la comunicación de otros dispositivos en las redes inalámbricas, que es también una especie de ataque de denegación de servicio (DoS) por inundación de asociación.
- ✓ El hombre en el ataque medio, el atacante se disfraza como un dispositivo que ya está en conexión directa con otro dispositivo. Luego, puede escuchar la comunicación en curso, inyectar información falsa o manipulada, o interceptar completamente la comunicación.

El ataque de sumidero es el ataque más arriesgado. No solo atrae todo el tráfico hacia la estación base, sino que también el atacante puede iniciar otras amenazas, como el reenvío selectivo, la alteración o la eliminación de paquetes.

7.3 Ataques de Software

En esta categoría, el atacante realiza el ataque mediante el uso de malware para robar datos, negar los servicios, etc.

Ataques de denegación de servicio (DoS). Existen tres tipos bien conocidos de ataques DoS contra nodos informáticos de borde: agotamiento de la batería, privación del sueño y ataques de interrupción. A continuación, describimos cada uno.

- ✓ Descarga de la batería: debido a limitaciones de tamaño, los nodos generalmente tienen que transportar baterías pequeñas con una capacidad de energía muy limitada. Esto ha convertido a los ataques de agotamiento de la batería en un ataque muy poderoso que indirectamente puede tener graves consecuencias, como la interrupción de un nodo o la falta de notificación de una emergencia. Por ejemplo, si un atacante puede encontrar una manera de agotar la batería de un detector de humo, podrá desactivar el sistema de detección de incendios. Un ejemplo de un ataque de agotamiento de la batería es cuando un atacante envía una cantidad considerable de paquetes aleatorios a un nodo y lo obliga a ejecutar sus mecanismos de verificación, por ejemplo, mecanismo de autenticación.
- ✓ Privación del sueño: la privación del sueño es un tipo específico de ataque DoS en el sentido de que la víctima es un nodo alimentado por batería con una capacidad de energía limitada. En este tipo de ataque, el atacante intenta enviar un conjunto no deseado de solicitudes que parecen ser legítimas. Por lo tanto, la detección de este tipo de ataque es mucho más difícil que la de un simple ataque de agotamiento de la batería.

- ✓ Ataques de interrupción: la interrupción del nodo de borde se produce cuando un dispositivo de borde deja de realizar su funcionamiento normal. En algunos casos, un conjunto de dispositivos o un dispositivo de administrador pueden dejar de funcionar. La interrupción puede ser el resultado de un error involuntario en el proceso de fabricación, el agotamiento de la batería, la falta de sueño, la inyección de código o el acceso físico no autorizado al nodo. Uno de los ejemplos más famosos de ataques de interrupción es inyectar (Stuxnet, 2010) en el programa de control de procesos nucleares de Irán. Stuxnet manipula las señales del sensor de control de procesos industriales de modo que el sistema infectado pierde su capacidad de detectar comportamientos anormales. Por lo tanto, el sistema no se apaga incluso en una situación de emergencia.

El ataque de gusanos es considerado el más inseguro. Los gusanos son probablemente la forma más destructiva y peligrosa de malware en Internet. Es el programa de autorreplicación que daña la computadora al usar agujeros de seguridad en el software y hardware de redes. Puede eliminar los archivos en el sistema, roba la información como contraseñas, también pueden cambiar las contraseñas sin su aviso, provoca bloqueos en la computadora, etc.

7.4 Ataques de Cifrado

Estos ataques dependen de destruir la técnica de encriptación y obtener la clave privada.

- ✓ Ataque de canal lateral, el atacante utiliza la información del canal lateral que se emite al cifrar los dispositivos. No es ni el texto simple ni el texto cifrado, contiene información sobre la potencia, el tiempo necesario para realizar la operación, la

frecuencia de fallas, etc. El atacante utiliza esta información para detectar la clave de cifrado.

- ✓ Ataques de criptoanálisis, en este ataque el adversario obtiene la clave de cifrado utilizando texto simple o texto cifrado. Según la metodología utilizada, existen diferentes tipos de ataques de criptoanálisis.
- ✓ Ataque de solo texto cifrado, en este caso, el atacante puede acceder al texto cifrado y determinar el texto plano correspondiente.
- ✓ Ataque de texto simple conocido, en este método, el atacante conoce el texto en claro para algunas partes del texto cifrado; el objetivo es descifrar la parte restante del texto cifrado utilizando esta información.
- ✓ Ataque elegido de texto simple, el atacante puede elegir qué texto sin formato está cifrado y encontrar la clave de cifrado.
- ✓ Ataque de texto cifrado elegido, al usar el texto plano del texto cifrado elegido, el atacante puede encontrar la clave de cifrado.
    - ✓ Ataque hombre en medio, cuando dos usuarios intercambian la clave, el atacante intercepta la comunicación y la obtiene.

Por ataque de cifrado, El ataque de canal lateral es el más difícil de manejar. Es muy difícil de detectar porque el atacante usa la información del canal lateral para realizar el ataque.

Muchos de los ataques a IoT descritos y clasificados anteriormente pueden evitarse manteniendo alguna precaución de seguridad como verificar la identidad del nodo mientras se realiza la comunicación, sin embargo, algunos de los ataques conocidos que son difíciles de detectar o prevenir han tenido la necesidad de encontrar una solución segura y eficiente.

Capitulo VIII: Contramedidas a vulnerabilidades Iot

La seguridad de IoT es un tema de investigación en curso que atrae cada vez más atención en la investigación académica, industrial y gubernamental. Muchas organizaciones en todo el mundo y corporaciones multinacionales están involucradas en el diseño y desarrollo de sistemas basados en IoT (Zaheer, 2012) para proporcionar una gran cantidad de servicios confiables, los diseñadores enfrentan varios desafíos, en particular, en las áreas de investigación relacionadas con la seguridad. Actualmente, varios esfuerzos de investigación intentan descubrir posibles amenazas y proporcionar contramedidas contra ellas.

8.1 Nodos de borde

Mecanismos basados en políticas y sistemas de detección de intrusiones (IDS). Los enfoques basados en políticas son mecanismos prometedores para resolver problemas de seguridad y privacidad en este nivel de IoT. La violación de las políticas esenciales se puede detectar continuamente mediante la introducción de un IDS quien asegura que las reglas generales no se rompan. Proporciona un enfoque confiable para defenderse contra el agotamiento de la batería y los ataques de privación del sueño mediante la detección de solicitudes inusuales al nodo. Varios esfuerzos de investigación recientes y en curso proporcionan diseños IDS eficientes para monitorear los nodos de borde y detectar posibles amenazas (Agrawal, 2004).

Asegurar la actualización de firmware. Cada actualización de firmware se puede iniciar de forma remota o directa. En el caso de la actualización remota de firmware, la base o el servidor emite un comando (CMD) para anunciar que hay una nueva versión de firmware disponible. Luego, un nodo con el nuevo firmware difunde un anuncio (ADV) a los nodos vecinos. Los nodos que están dispuestos a actualizar su firmware y también han recibido ADV comparan la nueva versión con su versión existente y envían solicitudes (REQ) si necesitan una actualización. Finalmente, el anunciante comienza a enviar datos a los solicitantes. Proporcionar un método seguro para actualizar remotamente el firmware requiere autenticación de CMD, ADV, REQ y paquetes de datos. Además de las actualizaciones remotas de firmware, algunos nodos admiten actualizaciones directas del firmware, por ejemplo, utilizando un cable USB. En este caso, debe verificarse la integridad del firmware, y el usuario, que intenta actualizar el firmware, debe autenticarse, porque la falta de mecanismos de verificación de integridad suficientes puede permitir que un atacante reemplace el firmware legítimo del dispositivo con uno malicioso.

8.2 Etiquetas RFID

Soluciones y sugerencias para abordar ataques contra etiquetas RFID.

- ✓ **Comando dormir**. Una etiqueta RFID tiene un PIN único, por ejemplo, una contraseña de 32 bits. Al recibir el PIN correcto del lector RFID, la etiqueta se puede eliminar, es decir, la etiqueta no podrá transmitir más información después de recibir este comando (Hernandez-Castro, 2006). Existe un enfoque alternativo llamado comando de suspensión que pone las etiquetas en suspensión, es decir, las desactiva durante un período de tiempo (Jules, 2006). Aunque estas ideas parecen simples a

primera vista, el diseño e implementación de esquemas de administración de PIN seguros y efectivos requieren técnicas sofisticadas.

- ✓ **El aislamiento**. Una forma muy efectiva de proteger la privacidad de las etiquetas es aislarlas de todas las ondas EM. Una forma es construir y usar salas de aislamiento. Sin embargo, construir tales habitaciones suele ser muy costoso. Un enfoque alternativo es utilizar un contenedor de aislamiento que generalmente está hecho de una malla metálica. Este contenedor, que puede bloquear las ondas EM de ciertas frecuencias, se llama jaula de Faraday. Otro enfoque es bloquear todos los canales de radio cercanos utilizando un bloqueador de RF activo que interrumpe continuamente canales de RF específicos.

- ✓ **Estimación de distancia**. El uso de la relación señal / ruido como métrica para determinar la distancia entre un lector y una etiqueta se propone en (Juels, 2006). Afirma que es posible derivar una métrica para estimar la distancia de un lector que intenta leer la información de la etiqueta. Esto permite que la etiqueta solo proporcione información basada en la distancia. Por ejemplo, la etiqueta puede liberar información general, como el tipo de producto, cuando se escanea a una distancia de 10 metros, pero libera su identificador único a menos de 1 metro de distancia.

- ✓ **Cifrado**: el cifrado completo generalmente requiere un hardware significativo. Por lo tanto, su implementación en etiquetas RFID no ha sido factible debido a la necesidad de que las etiquetas sean de bajo costo. Para una implementación estándar de AES,

normalmente se necesitan puertas de 20-30K, mientras que las etiquetas RFID solo pueden almacenar cientos de bits y son compatibles con puertas lógicas de 5-10K. Las limitaciones derivadas del recuento de puertas y el costo sugieren que la etiqueta solo puede dedicar 250-3500 puertas al mecanismo de seguridad. Hasta ahora no se ha implementado una versión completamente desarrollada de AES en ninguna etiqueta RFID.

8.3 Soluciones para problemas de seguridad en la comunicación.

Se han propuesto muchos protocolos de enrutamiento de red de sensores, pero ninguno de ellos se ha diseñado con la seguridad como objetivo.

Enrutamiento confiable. Una característica esencial de las redes IoT que complica la implementación de protocolos de enrutamiento seguro es que los nodos o servidores intermedios pueden requerir acceso directo al contenido del mensaje antes de reenviarlo. Se han propuesto varios ataques válidos contra el enrutamiento en (Wagner, 2003) donde abordan la mayoría de los principales escenarios de ataque y proporcionan el primer análisis de seguridad detallado de los principales protocolos de enrutamiento y ataques prácticos contra ellos, junto con contramedidas.

IDS. IDS es esencialmente necesario a nivel de comunicación como una segunda línea de defensa para monitorear las operaciones de red y los enlaces de comunicación, y generar una alerta en caso de cualquier anomalía, por ejemplo, cuando se ignora una política predefinida. Los enfoques IDS tradicionales generalmente se personalizan para WSN o para Internet

tradicional. Sin embargo, pocas propuestas recientes de IDS abordan las preocupaciones de seguridad y privacidad de IoT directamente. SVELTE (S. Raza, 2013) es uno de los primeros IDS diseñados para cumplir con los requisitos de los nodos de IoT conectados a IPv6. Es capaz de detectar ataques de enrutamiento, como información falsificada o alterada, y un ataque de Black Hole. Otro método de detección de intrusos para el IoT se ha propuesto en (Caiming Liu, 2011). Manifiestan los autores que se construye el método de aplicación basado en la teoría inmune donde los elementos de detección en el entorno evolucionan dinámicamente para simular los mecanismos de auto adaptación y autoaprendizaje.

Esquemas criptográficos. El uso de esquemas criptográficos, por ejemplo, encriptación fuerte, para proteger los protocolos de comunicación es una de las defensas más efectivas contra una variedad de ataques, incluyendo escuchas y ataques de enrutamiento simples, a nivel de comunicación. Se han propuesto métodos de encriptación para abordar problemas de seguridad en la comunicación (J Daemen, 2013). Las técnicas de cifrado-descifrado, desarrolladas para redes cableadas tradicionales, no son directamente aplicables a la mayoría de los componentes de IoT, en particular, a pequeños nodos de borde alimentados por batería. Los nodos de borde suelen ser sensores pequeños que tienen una capacidad limitada de batería, potencia de procesamiento y memoria. El uso de cifrado aumenta el uso de memoria, el consumo de energía, el retraso y la pérdida de paquetes. Las variantes de AES han arrojado resultados prometedores para proporcionar una comunicación segura en IoT. Además, se han propuesto diferentes métodos de encriptación livianos, por ejemplo, PRESENT (Vaithiyanathan, 2017) . Desafortunadamente, en este momento, no existen métodos prometedores de cifrado de clave pública que brinden suficiente seguridad y cumplan con los requisitos livianos.

Autorización basada en roles. Para evitar una respuesta a las solicitudes de intrusos o nodos maliciosos en el sistema, un sistema de autorización basado en roles verifica si un componente, por ejemplo, nodo de borde, proveedor de servicios o enrutador, puede acceder, compartir o modificar la información. Además, para cada comunicación, el sistema de autorización debe verificar si las dos partes involucradas en la acción han sido validadas y si requieren autoridad (Vaish, 2011).

Muy recientemente, (A. Ouaddah, 2017) presentaron una evaluación cuantitativa y cualitativa de las soluciones de control de acceso disponibles para IoT. Los autores destacaron cómo cada solución logró varios requisitos de seguridad, señalando que la adopción de enfoques tradicionales no se puede aplicar directamente a IoT en muchos casos. Los autores también declararon que los enfoques centralizados y distribuidos podrían complementarse entre sí al diseñar el control de acceso adaptado a IoT.

Actualmente no se cuenta con un mecanismo o estándar de seguridad específico para diferentes dispositivos y su interoperabilidad. Se espera que los ataques nuevos o variantes aumenten a medida que se generen paquetes de varios patrones desde numerosos dispositivos, y por lo tanto se requiere un gran esfuerzo de investigación para resolver estos problemas.

Capitulo IX: Algoritmos de criptografía para IoT

La criptografía ha sido un componente de seguridad de las redes e Internet durante mucho tiempo, es útil para evitar que la información y los datos privados se recopilen y difundan a aquellas personas o grupos sin los privilegios adecuados para acceder a los datos. La criptografía se ha utilizado mucho en redes típicas para comunicaciones seguras e intercambio de datos.

Los algoritmos criptográficos están diseñados alrededor de suposiciones computacionales de dureza que hacen que esos algoritmos sean difíciles de romper por cualquier adversario. Sin embargo, teóricamente es posible romper un sistema, pero lo que se ha logrado es que no es factible hacerlo en un corto período de tiempo. Estos esquemas son por lo tanto llamados computacionalmente seguros.

En cuanto a IoT, los dispositivos sensores tienen un tamaño de memoria limitado, velocidad de procesamiento y suministro de energía. Por lo tanto, el algoritmo criptográfico para IoT debe desarrollarse teniendo en cuenta estas restricciones. El objetivo del algoritmo debe ser garantizar el cifrado y la integridad. Dado que los nodos sensores tienen memoria y potencia de procesamiento limitadas, el algoritmo no debería estar más orientado al software. Algunos criptosistemas basados en IoT se describen:

En 2007, el investigador (Martin Hell, 2007) introdujo Grain, un cifrado de flujo que brinda seguridad más alta que otros algoritmos como E0 y A5 / 1. Está diseñado para usar poco hardware. Un nuevo algoritmo considerado adecuado para implementar en dispositivos con recursos limitados como etiquetas RFID. estas etiquetas contienen memoria y potencia limitadas,

y otros algoritmos como AES que necesita una gran cantidad de equivalentes de puerta, por lo tanto, este algoritmo no puede aplicarlo en tales etiquetas.

En 2010, los investigadores (Yiyuan Luo, 2010) introdujeron un cifrado de flujo ligero (WG-7). Este sistema se comparó con otros algoritmos en varias plataformas y mostró que (WG-7) se puede ejecutar de manera eficiente para aplicaciones (RFID). Se considera un candidato nuevo y competitivo para las aplicaciones RFID.

En 2010 los autores (Jesus Ayuso, 2010) consideraron dispositivos basados en 6LoWPAN, que ha definido nuevos desafíos de seguridad. La criptografía de clave simétrica (criptografía de clave privada) utilizada en las redes inalámbricas de sensores, pero no es apta para IoT, por cuanto la clave privada no es escalable. Los estudios sobre la seguridad de las redes de sensores están demostrando resultados esperanzadores como implementaciones eficientes de criptografía de clave asimétrica (criptografía de clave pública). En el artículo, los autores propusieron que el desplazamiento de bits implemente la operación de multiplicación para la criptografía de curva elíptica (ECC) y (RSA) en lugar de la operación de multiplicación del microprocesador.

Los Investigadores (Zheng Gong, 2012) , presentaron KLEIN, una nueva familia de cifrados de bloques ligeros. Fue diseñado para dispositivos con recursos limitados como etiquetas WS y RFID. KLEIN se centró en la implementación de software, también es eficiente en hardware y tiene diferentes tamaños de clave. A su vez los investigadores (Xinxin Fan, 2012) presentaron un cifrado de flujo WG-8 para proporcionar seguridad en dispositivos con recursos limitados como RFID, Nodos de sensores inalámbricos, tarjetas inteligentes. Este algoritmo liviano (WG-

8) es inmune a ataques bien conocidos contra cifrados de flujo y tiene un buen rendimiento y consume poca energía.

Para el año 2014 los autores (Huqing Wang, 2014) presentaron una mejora de EIGamal basada en ECC. Este algoritmo puede mejorar la seguridad y extender el uso de EIGamal basado en ECC. Se aplicó principalmente para mejorar la seguridad de las aplicaciones IoT.

En 2014, los autores (HakJu Kim, 2014) introdujeron un conocido esquema de cifrado ligero, PRINCE. Los autores se centraron en la metodología para extender el tamaño del bloque y el tamaño de la clave de PRINCE. El objetivo del autor era diseñar un esquema de cifrado liviano sin inversión especializado para IoT y para correr con las características:

- ✓ a una alta velocidad de ejecución
- ✓ con bajo uso de área de chip de hardware
- ✓ con bajo consumo de energía
- ✓ tamaño de bloque flexible a 128 bit
- ✓ tamaño de clave flexible a 128, 192, 256 bit
- ✓ con seguridad comprobable.

En este año también se presentó el Cifrado basado en atributos (ABE), una solución común para proporcionar seguridad de transmisión de datos, uso compartido y almacenamiento en el entorno extendido como IoT. Pero ABE se basa en un emparejamiento bilineal que lo hace inadecuado para dispositivos con recursos limitados en IoT. Los autores del cifrado (Xuanxia Yaoa, 2014) propusieron que ABE sin emparejamiento confíe en la criptografía de curva elíptica (ECC) para etiquetar los problemas de seguridad y privacidad en IoT.

Los investigadores (Ray Beaulieu, 2015) presentaron a las familias SIMON y SPECK como cifrado de bloque ligero diseñado por (NSA). Solía proporcionar seguridad en un entorno restringido donde AES no es factible. Simon y Speck admiten un gran tamaño de bloque y clave, en comparación con los cifrados de bloque ligeros existentes. A su vez (Tuhin Borgohain, 2015) tenía como objetivo realizar un estudio con un análisis comparativo de varias bibliotecas de criptografía que se pueden aplicar en el campo IoT. En este artículo, los autores concluyeron que no existe una biblioteca única que pueda ser adecuada para los dispositivos IoT que nos rodean. Por último los autores (Bai T Daisy Premila, 2015) propusieron un nuevo marco de seguridad basado en ECC para IoT y Cloud Computing. La criptografía de curva elíptica es un excelente criptosistema para un entorno de IoT y computación en la nube. Requiere menos cómputo y tamaño de memoria y también proporciona más seguridad. El ECC de 160 bits ofrece una seguridad equivalente al RSA de 1024 bits.

Los autores (Wei Li, 2016) en 2016 mostraron un análisis de seguridad de TWINE, un nuevo criptosistema ligero de Estructura Generalizada de Feistel (GFS) en IoT. Ese estudio explicó que TWINE es flexible para implementar seguridad para RFID, tarjetas inteligentes y otros dispositivos altamente restringidos. En ese mismo año (M.R. Balasubramaniam, 2016) propusieron EECC (criptografía de curva elíptica EIGamal) es un nuevo método eficiente para cifrar y descifrar un texto utilizando el valor de ASCII hexadecimal para cada carácter. Aunque, ECC tiene un tamaño de clave corto brinda la misma seguridad en comparación con otros sistemas criptográficos como RSA. Estas características han hecho que la criptografía de curva elíptica sea efectiva en algunas aplicaciones, como dispositivos móviles, tarjetas inteligentes, tarjetas con chip y comercio electrónico.

IoT contiene datos confidenciales de un objeto físico, como nombres y direcciones de personas, etc., por lo tanto, la seguridad de la transmisión de datos a través de IoT es una tarea necesaria y desafiante. Los requisitos de seguridad de IoT coinciden con las redes tradicionales, por lo tanto; parámetros como integridad, confidencialidad, autenticidad y disponibilidad son necesarios para proporcionar seguridad al entorno de IoT; Debido a restricciones en dispositivos restringidos que se utilizan en redes IoT, no se puede implementar todo el diseño de soluciones de seguridad para redes tradicionales directamente en IoT.

El esquema de diseño para proporcionar seguridad para recursos limitados debe ser un esquema ligero. Los dispositivos restringidos requieren algoritmos criptográficos adecuados para adaptarse a sus características y esto puede considerarse como un gran desafío.

Actualmente, los algoritmos criptográficos disponibles necesitan un análisis más amplio para determinar su aplicabilidad en IoT. Para implementar estos algoritmos en dispositivos restringidos de IoT inciertos se requieren más análisis para garantizar la aplicabilidad de estos en recursos restringidos (memoria, velocidad del procesador) en el entorno de IoT.

Capitulo X: Protocolo 5G, características y tendencias para IoT

A medida que el IOT aumenta su popularidad, es necesaria una tecnología de comunicación móvil inalámbrica, más allá de 4G, que pueda soportar grandes cantidades de transmisión de datos de manera eficiente y con un ancho de banda muy alto. En un futuro cercano, es decir, dispositivos IOT de próxima generación, algunos de los principales objetivos o demandas que deben abordarse son el aumento de la capacidad, la velocidad de datos mejorada y la latencia disminuida. El desarrollo de la tecnología de comunicación 5G promete satisfacer las necesidades de arquitecturas complejas de IOT.

La actual tecnología 4G depende del llamado acceso múltiple ortogonal. Tal acceso múltiple ortogonal será difícil de soportar para futuras aplicaciones dada la enorme cantidad de dispositivos para los cuales se debe asignar espacios de tiempo dedicados a cada uno de ellos, de ahí que la cantidad de intervalos de tiempo disponibles y los recursos de ancho de banda serán insuficientes. Es por eso que el acceso ortogonal múltiple no funcionará para el 5G. El inconveniente de la arquitectura 4G es que puede admitir un ancho de banda máximo de 1 Gigabit y, a medida que aumenta el ancho de banda requerido por los dispositivos IOT, 4G puede convertirse en un cuello de botella. De otra parte, 4G puede ser vulnerable a los piratas informáticos y los virus. Como la seguridad de los datos y el ancho de banda son más importantes para los dispositivos IOT, 4G pronto no será adecuado para los dispositivos IOT.

En comparación con los sistemas 4G, los sistemas celulares 5G son un salto para frecuencias más altas donde es más fácil obtener anchos de banda más amplios.

La llegada de 5G, supone será la columna vertebral para el ecosistema IOT. Los ecosistemas IOT habilitados para 5G pueden proporcionar una infraestructura sostenible para un mayor desarrollo de esos ecosistemas IOT.

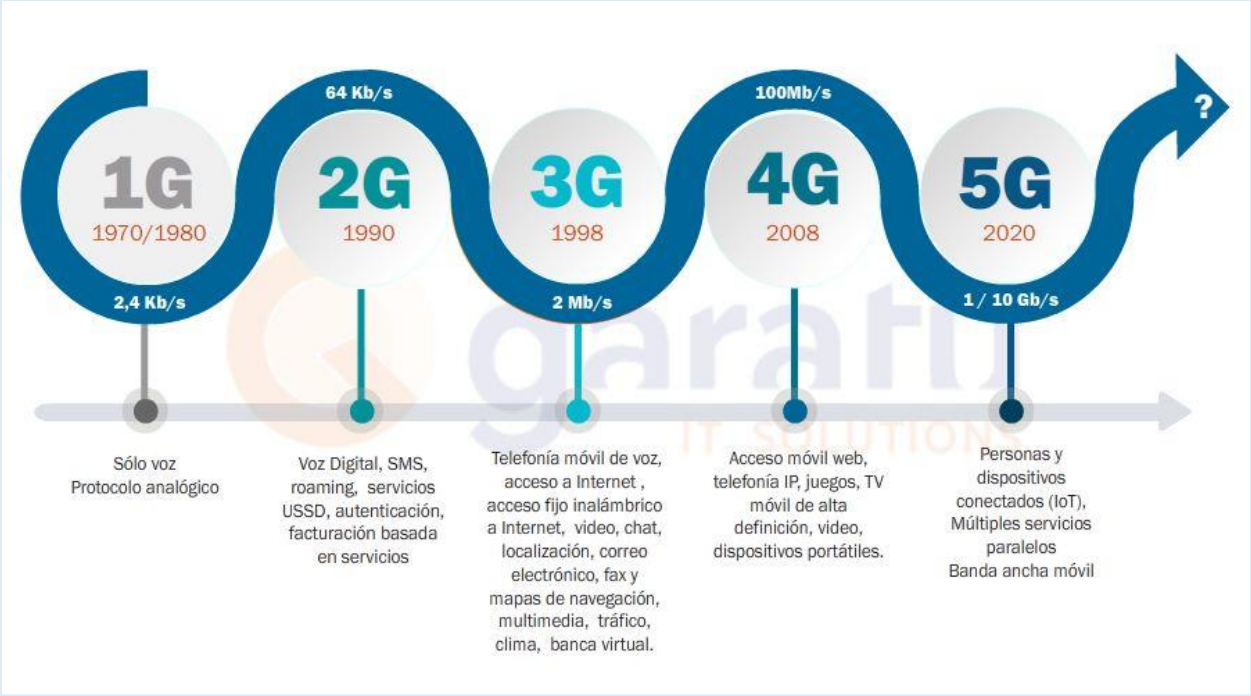

Figura 8 Las 5 Generaciones de las conexiones inalámbricas
(Fuente: https://grupogaratu.com/tecnologia-5g-que-es-como-beneficia-industria-4-0-iot/)

El desarrollo de la tecnología inalámbrica de 5ta generación (5G) promete un ancho de banda que antes se había experimentado. 5G promete tener más velocidad, capacidad y bajo costo por bit. Proporcionará una gran capacidad de transmisión de hasta Gigabit que admite casi 65,000 conexiones a la vez y promete ser más seguro que 4G. Dado que la mayor parte del espectro asignado a la IoT no tiene licencia y tiene una banda de frecuencia limitada, varias redes de IoT pueden coexistir en la misma banda de frecuencia para generar interferencia mutua. Por lo tanto, con el rápido crecimiento de los usuarios y las empresas inalámbricas, el desarrollo de IoT se ha visto restringido por la escasez de recursos de espectro en gran medida (X Chen, 2017) . Sin

embargo, el espectro con licencia, como las bandas de frecuencia para comunicaciones de evolución a largo plazo (LTE) y de quinta generación (5G), son capaces de proporcionar garantías de QoS altas en áreas amplias, ya que los operadores pueden evitar interferencias y controlar los niveles de uso. Como resultado, combinar IoT y 5G puede ser una buena opción para los futuros servicios de IoT que requieren transferir una gran cantidad de datos de alta calidad (Lin, y otros, 2017), (X Liu, 2017).

la tecnología 5G se basará en:

- ✓ Acceso de radio económico similar a la fibra que alcanza velocidades de datos superiores a 10 Gb / s, mediante el uso de bandas de frecuencia más altas por encima de 6 GHz y tecnologías relacionadas.
- ✓ Network Function Virtualization (NFV), permitirá implementar funciones de red específicas en software que se ejecuta en hardware genérico sin la necesidad de costosas máquinas específicas de hardware. Reducción de costos de implementación, administración y operación; Permitir reutilizar y compartir la misma funcionalidad entre clientes.
- ✓ Las redes definidas por software (SDN) permitirán que el control de los recursos de la red se abra a terceros, flexibilidad para acomodar aplicaciones exigentes de nivel profesional.

Los requisitos básicos de las aplicaciones 5G que están fuera de las capacidades actuales de la tecnología 4G serán:

- ✓ baja latencia de 1 ms (10 a 20 ms para 4G).
- ✓ sirviendo 1 millón de dispositivos / km (alrededor de 1000 dispositivos / km para 4G)
- ✓ despliegue rápido de nuevos servicios en 1 hora (hecho en días con la tecnología actual)

10.1 Tecnologías habilitadoras redes 5G

Varios trabajos en la literatura exploran la relación entre las redes IoT y 5G, principalmente desde el punto de vista de las empresas de telecomunicaciones y desde los requisitos de comunicación.

(M. R. Palattella, 2016) analizaron el potencial de las tecnologías 5G para el IoT, considerando aspectos tanto tecnológicos como de estandarización. En su artículo, revisaron el panorama contemporáneo de conectividad IoT (como, Zigbee, Bluetooth Low Energy, LP-Wifi), así como las características principales que pueden permitir un uso extendido y conveniente de los sistemas 5G para IoT. En particular, imaginaron la necesidad de desacoplar enlaces descendentes / ascendentes y proporcionar tanto un acceso asistido por licencia como una red de acceso por radio como servicio. Además, identificaron las redes definidas por software (SDN) y la virtualización de funciones de red (NFV) como los principales habilitadores de red 5G.

Entre los habilitadores de 5G, la comunidad de investigación estudió a fondo el uso de SDN para las tecnologías 5G e IoT. (F. Granelli, 2015) reconoció que SDN, con su capacidad de enrutar de manera inteligente el tráfico de Internet y usar eficientemente los recursos de la red, permitirá eliminar los cuellos de botella y un procesamiento eficiente de los datos generados por las aplicaciones de IoT, sin forzar la red. Las capacidades SDN de cambio de servicio, calendario de ancho de banda y gestión de carga dinámica, en particular, serán particularmente útiles para el IoT. En el lado 5G.

Las redes definidas por software y 5G, una combinación de redes definidas por software (SDN) y virtualización de funciones de red (NFV), es un área importante que tiende a hacer que los servicios y aplicaciones de IoT sean más flexibles.

10.1.1 Virtualización de funciones de red (NFV)

La virtualización de funciones de red (NFV) desacopla las funciones de red del hardware subyacente y las centraliza en los servidores de red, lo que hace que la arquitectura de la red sea altamente flexible a partir de una reconfiguración rápida y adaptativa (I.F. Akyildiz, 2015). Dichas funciones de red podrían ser servicios de IoT virtualizados para cualquier tipo de áreas diversas, IoT para ciudades inteligentes, transporte público, incluso en dominios de atención médica. La diversidad y las necesidades avanzadas de esos servicios podrían gestionarse fácilmente mediante la transformación a NFV y la implementación de las aplicaciones en un entorno definido por software. Como se indica en (Samdanis, 2017), hay muchas características clave de NFV / SDN, tecnología virtualizada y computación en la nube en general: bajo demanda para autoservicio, amplio acceso a la red, agrupación de recursos, elasticidad rápida y medición de servicios. Sin embargo, un conjunto de atributos que tienen un impacto significativo en la ecuación OPEX incluye: elasticidad automatizada, independencia de software y hardware, multipropiedad y agrupación de recursos, uniformidad de hardware, infraestructura de software virtualizado, racionalización del proceso de operaciones, etc. Además, vale la pena mencionarlo. El hecho de que con la transición a NFV / SDN, se espera que muchos proveedores de servicios realineen las operaciones de la red para admitir un modelo operativo en el que los servicios de red y los recursos de red se gestionen de manera eficiente.

10.1.2 Redes definidas por software

SDN es un enfoque de arquitectura de red que permite que la red sea controlada de forma inteligente y centralizada, o 'programada', utilizando aplicaciones de software. También tiene como objetivo hacer que la red sea tan ágil y flexible como el servidor virtualizado y la infraestructura de almacenamiento de los centros de datos modernos. El objetivo de SDN es permitir que los ingenieros y administradores de redes respondan rápidamente a los cambiantes requisitos comerciales. SDN brinda facilidad de programación para cambiar las características de redes enteras. Esto simplifica la gestión de la red, ya que está desacoplada del plano de datos. Por lo tanto, los operadores de red pueden administrar, configurar y optimizar los recursos de red de manera fácil y rápida con programas dinámicos, automatizados y sin propiedad.

La virtualización de funciones de red, se puede implementar sin que se requiera un SDN. Sin embargo, la combinación de las tecnologías antes mencionadas puede mejorar el rendimiento, simplificando la compatibilidad de diferentes servicios de IoT con requisitos en conflicto, y facilita los procedimientos de operación y mantenimiento al mismo tiempo (T. Kuo, 2018).

5G es una de las tecnologías inalámbricas más sofisticadas desarrollada hasta ahora. Revolucionará toda el área donde la red inalámbrica se puede utilizar para una comunicación eficiente. Aunque las especificaciones de 5G siguen siendo inestables, se predice que la próxima generación de tecnología móvil beneficiará en gran medida la innovación de IoT. Se espera que las redes 5G proporcionen velocidades más rápidas, latencia reducida y soporte de red para aumentos masivos en el tráfico de datos provenientes de diferentes y numerosos dispositivos IoT.

10.1.3 Comunicación de dispositivo a dispositivo (D2D)

La tecnología D2D permite la comunicación directa entre dos dispositivos móviles sin la ayuda de la estación base y otras infraestructuras de red, es utilizado ampliamente en IoT para mejorar el rendimiento de la red, reducir el consumo de energía y superar la escasez de espectro.

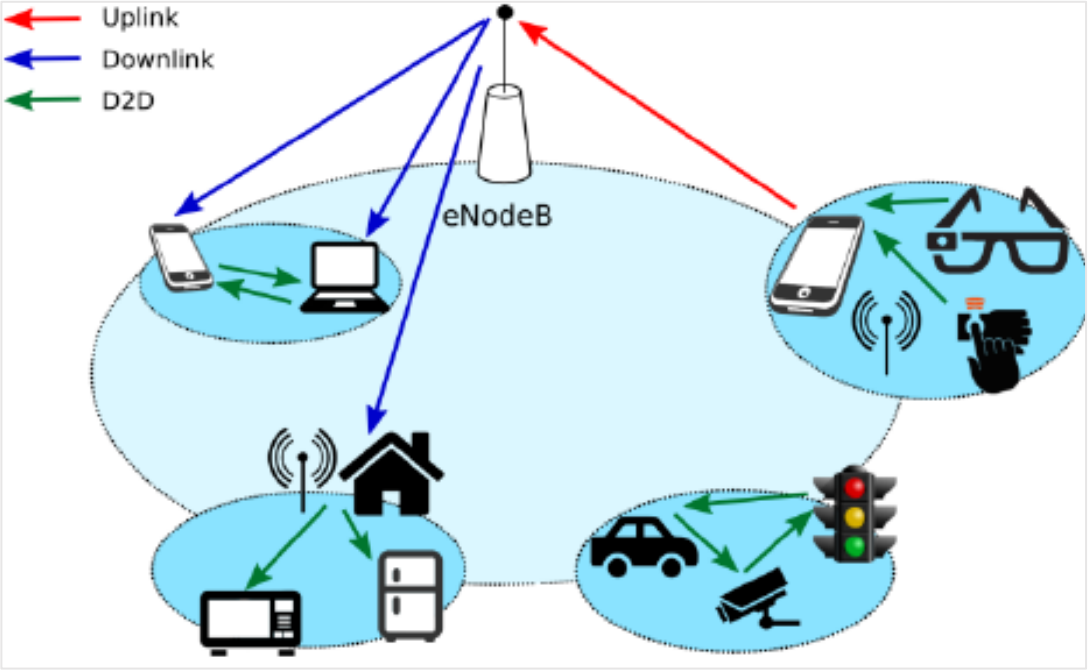

Figura 9 Escenarios de comunicación D2D
(Fuente: https://www.researchgate.net/figure/D2D-communications-in-5G-IoT-networks_fig1_283327011)

Los estándares IEEE 802.11 y 802.15 proporcionan protocolos para la comunicación D2D, como Wi-Fi, LTE y Bluetooth. Sin embargo, debido a los problemas de seguridad de los protocolos inalámbricos, la comunicación D2D requiere mejorar aspectos como, manipulación de información, suplantación de nodos y reproducción de mensajes.

Por lo general los esquemas de cifrado, como el Estándar de cifrado de datos (DES) y el Estándar de cifrado avanzado (AES) se utilizan para resistir el ataque de espionaje de mensajes. Sin embargo, se requiere una clave segura para compartir previamente entre usuarios legítimos

cuando se utilizan esquemas de cifrado y protocolos de autenticación de mensajes para una comunicación segura. Es crucial en la comunicación D2D segura generar y distribuir una clave segura.

Tradicionalmente, el método basado en terceros de confianza (por ejemplo, el protocolo Kerberos), y el método basado en la clave pública (por ejemplo, el protocolo Diffie-Hellman) se utilizan para distribuir una clave segura; sin embargo, cuando estos esquemas cumplen con la comunicación D2D, enfrentan problemas como.

- ✓ La dificultad para generar y distribuir una clave con la ayuda de un tercero debido a la movilidad de los dispositivos inalámbricos en escenarios de comunicación D2D.
- ✓ Los métodos de distribución de claves basados en claves públicas requieren una alta capacidad de computación y consumo de energía, mientras que los dispositivos inalámbricos tienen una capacidad de computación y energía limitada por cuanto la mayoría de ellos funcionan con baterías.

Por lo tanto, un sistema de comunicación D2D seguro con un método de distribución de claves ligero y eficiente es la piedra angular para la amplia aplicación de la comunicación D2D.

10.1.4 Comunicación tipo maquina M2M

La comunicación máquina a máquina, también llamada comunicación M2M o comunicación tipo máquina (MTC), utiliza dispositivos como sensores y medidores para capturar un evento o datos como temperatura, presión y consumo de gas o agua. Los datos capturados se envían a través de una red cableada o inalámbrica al servidor / aplicación que traduce los eventos

capturados en información significativa para el usuario. En otras palabras, a diferencia de la comunicación de máquina a persona, una comunicación de máquina a máquina es información intercambiada a través de una red cableada o inalámbrica o híbrida, con una interacción humana mínima o nula.

M2M se refiere a numerosas aplicaciones y escenarios. La medición inteligente, el monitoreo remoto de la salud y la operación de rescate ante desastres son algunas de las aplicaciones importantes de la comunicación M2M. Se requiere que los dispositivos M2M envíen periódicamente o bajo pedido datos monitoreados al servidor M2M. Debido a su amplia cobertura y redes heterogéneas (HetNets), se espera que la tecnología 5G admita, además del tráfico tradicional de voz y datos, la comunicación M2M.

La comunicación D2D se puede diferenciar con la comunicación máquina a máquina (M2M), por cuanto este último establece una comunicación de datos entre máquinas o dispositivos que no requieren mediación humana ni imponen restricciones específicas en los rangos de comunicación y se basa en redes tradicionales como 3G y LTE, es esencialmente una tecnología orientada a la aplicación. La comunicación D2D, por otro lado, supone una proximidad cercana entre los dispositivos y se basa solo en las capacidades del dispositivo local sin soporte de infraestructura centralizada. Puede usarse para mejorar el rendimiento de la red y la calidad del servicio.

10.1.5 NB-IoT

3GPP introdujo en la versión 13 (2016) una nueva interfaz de radio dedicada a la comunicación masiva de tipo de máquina (mMTC), llamada Narrowband-IoT (NB-IoT), que

funciona en el espectro celular con licencia y es compatible con los sistemas LTE / LTE-A. Las características específicas de NB-IoT incluyen la aplicación de técnicas de mejora de cobertura, que se espera que proporcionen una mayor confiabilidad de conexión dentro de un área de cobertura extendida, en comparación con los sistemas 4G actuales. Dado que NB-IoT también se visualiza como el estándar 3GPP para el futuro IoT basado en 5G, el análisis de dicha tecnología parece de suma importancia.

10.1.6 Big Data Analytics

Los datos generados a través de IoT y big data están vinculados entre sí, la integración de big data con loT mejorará las operaciones en varios sectores como el sistema educativo moderno, el transporte inteligente, la protección del medio ambiente, la agricultura, ciudades inteligentes y muchos más.

El análisis de big data es un desafío importante para numerosas aplicaciones que requieren visualizar gráficos, cuadros y tablas para trabajar en la escalabilidad y la complejidad de los datos. Analizar las técnicas actuales de big data para organizaciones empresariales es el análisis de predicción, minería de datos y análisis estadístico. Las tecnologías actuales que se utilizan en la analítica de big data son Apache, Hadoop y herramientas asociadas como Map reduce, Pig, Hive, Spark, entre otras.

La competencia social de Big Data e IoT es la clave emergente para escalar la toma de decisiones. El estado actual de IoT es deficiente sin Big Data. Cualquier empresa antes de ingresar al IoT debe comprender la relación entre Big Data e IoT. Hasta ahora, la distribución de

IoT produce un impacto en la entrega de servicios y herramientas al recopilar la información de los sensores conectados y otros dispositivos.

IoT y Big Data Analytics presentan algunos desafíos en cuanto a:

- ✓ Privacidad, en el contexto de los grandes datos de IoT, la seguridad y la privacidad son los desafíos clave en el procesamiento y almacenamiento de grandes cantidades de datos. Además, para realizar operaciones críticas y alojar datos privados, estos sistemas dependen en gran medida de servicios e infraestructura de terceros. Por lo tanto, un crecimiento exponencial en la velocidad de datos causa dificultades para asegurar todas y cada una de las porciones de datos críticos.
- ✓ Minería de datos, los desafíos se relacionan con la extracción de los datos de una gran cantidad de estos, visualización y la integración de los datos.
- ✓ Integración, la integración de los datos es un problema más complejo y desafiante debido a la visión uniforme de la información que se obtiene de diferentes fuentes que pueden ser datos estructurados, no estructurados y semiestructurados.

10.1.7 Cifrado de datos de reposo

Para cumplir con dos requisitos de la CIA, la Confidencialidad y la Integridad, en un modelo tradicional de red es necesario cifrar los datos en tránsito, en uso y almacenados. Las contramedidas más usadas para proteger la integridad de los datos son el cifrado, la función criptográfica hash, firmas y certificados digitales, IDS, controles de versión, mecanismos seguros de autenticación y control de acceso. Así mismo, las contramedidas más usadas con el fin de proteger la confidencialidad son la clasificación y el etiquetado de la información; eficientes medidas de control de acceso y autenticación; cifrado de los datos en proceso, en tránsito y en

almacenamiento. Para fines de copia de seguridad es recomendable utilizar un control de versión.

Como se mencionó con anterioridad, IoT es una tecnología que ha heredado fallas del modelo tradicional de red y a su vez, los objetivos de seguridad típicos de la CIA se aplican a esta tecnología, se hace necesario cifrar los datos en reposo almacenados en discos rígidos, medios extraíbles o unidades USB.

El cifrado en reposo consiste en codificar la información almacenada mediante un algoritmo simétrico de manera que no pueda ser leída de forma transparente. Este método protege la información de la exposición y garantiza que los datos no se pueden leer, siempre que su clave de cifrado esté asegurada.

Para reducir el riesgo que representan los hackers, las amenazas internas y otros ataques maliciosos, grandes compañías usan cifrado de datos en reposo, es el caso de Microsoft en su producto Microsoft Azure, Google con Google Cloud Platform y Amazon con Amazon EMR.

Capitulo XI: Modelo propuesto

El modelo propuesto que a continuación se describe en la figura número 10 página 84, está compuesto por una sinergia tecnológica de 4 capas fundamentales y 3 subcapas derivadas de la capa Edge, el cual considera una arquitectura basada en la tecnología 5G, donde las capas 1, 2 y 3 integran el ecosistema IoT y estas a su vez se basan en una arquitectura combinada Edge / Gateway que se ilustra en la figura número 11, página 85.

Presenta características como, eficiencia, agilidad, simplicidad, seguridad y capacidad de respuesta a altas demandas de tráfico de datos, complementadas con la aplicación de buenas prácticas en ciber seguridad donde se consideró protección contra intrusiones maliciosas y datos almacenados con cifrado simétrico.

considerando las contramedidas a vulnerabilidades IoT planteadas en el capítulo VIII, el modelo aquí presentado contempla el uso de firewalls para verificar el tráfico entrante y saliente según las reglas requeridas y configuradas por quien considere el uso de ésta arquitectura, así como para restringir el acceso a servicios específicos y realizar modificaciones pertinentes a la funcionalidad deseada como otorgar acceso público al servidor web, pero evitar el acceso al telnet y a los otros demonios no públicos. Además del firewall, se considera de suma importancia el uso de un IDS por cuanto es una potente herramienta de seguridad que constantemente inspecciona toda la actividad de la red entrante y saliente. El IDS identifica cualquier patrón sospechoso que pueda indicar un ataque y actúa como un control de seguridad en todas las transacciones que tienen lugar dentro y fuera del sistema.

11.1 Capa Percepción

La capa física o de percepción involucra varios tipos de sensores de datos como RFID, códigos de barras o cualquier otra red de sensores. El objetivo de esta capa es obtener información del entorno mediante el uso de sensores y luego enviarla a la capa de red. Para mejorar la seguridad de esta capa, la próxima generación de microcontroladores debe admitir las características de seguridad como Funciones físicas no clonables (PUF). La solución a los problemas de seguridad en la capa de dispositivos consiste en el diseño de una arquitectura de seguridad eficiente en microcontroladores. Utilizando PUF se podría mitigar la falsificación del nodo de borde utilizando identificación precisa. Además, los diseñadores de microcontroladores deben incluir un mecanismo de acceso bien definido, fácil y seguro.

En esta capa es necesario asegurar la actualización de firmware de los nodos, un buen método para realizar este procedimiento se indica en el capítulo VIII, página 57 del presente documento. El IDS cumple una función en esta sección, la de proteger los nodos de borde para asegurar que las reglas generales no se rompan.

11.2 Capa de red

El objetivo de la capa de red consiste en transmitir los datos recopilados desde la capa de percepción a cualquier sistema de procesamiento de información específico a través de Internet, red móvil o cualquier otro tipo de red confiable. Las redes 6LoWPAN utilizan el protocolo IEEE 802.15.4 como capa de enlace. IEEE 802.15.4 y DTLS ofrecen la seguridad que requiere la capa de enlace. En esta capa se debe confiar en el nodo que participa en el proceso de comunicación.

En la capa de enlace se da la comunicación de dispositivo a dispositivo (D2D), la que se considera una técnica prometedora en las tecnologías de red celular 5G, los esquemas de retransmisión D2D presentan varias ventajas y pueden ayudar a mejorar la confiabilidad, la tolerancia a fallas y la escalabilidad del acceso a la red formando una red HetNet donde los nodos puedan comunicarse entre sí.

La seguridad en la capa de red, a nivel de comunicación, el IDS es esencialmente necesario como una segunda línea de defensa para monitorear las operaciones de red.

11.3 Capa Edge computing

La capa Edge se relaciona con servicios de analítica y de pre procesado que se ubican en el límite de la red. La analítica Edge ocurre en tiempo real (o casi en tiempo real) al procesar el flujo de datos en el punto en el que los datos se recopilan según llegan desde los sensores. Las tareas básicas de pre procesamiento, como el filtrado y la agregación de datos, se ejecutan en el límite y luego los datos principales pre procesados se transfieren en sentido ascendente hacia los servicios y aplicaciones de la nube. Esta capa se combina con la capa de enlace para configurar un modelo Edge / Gateway lo que permite mejorar la ciberseguridad, el almacenamiento y un procesamiento de datos más rápido.

En esta sección la seguridad se refuerza con el cifrado de datos en la transmisión, con el uso de conexiones VPN y monitorizando de forma exhaustiva el control de acceso.

11.3.1 Cloud computing

Después de preparar los datos se envían en sentido ascendente para procesarlos aún más, almacenarlos y utilizarlos dentro de las aplicaciones de la nube, en la nube las aplicaciones que realizan el procesado de datos, a menudo se complementan con aplicaciones móviles y con aplicaciones de clientes basadas en la web, que presentan los datos a los usuarios finales que brindan acceso a herramientas para explorar y analizar más a fondo, a través de paneles de instrumentos y de visualizaciones.

11.3.2 Cifrado de los datos en reposo

Para el modelo aquí propuesto se considera el uso de cifrado en reposo por cuanto proporciona protección para la información almacenada, está diseñado para evitar la exposición de los datos y para que un atacante acceder a ellos y leerlos. Otra importante característica de usar cifrado de datos en reposo consiste en acceder a la información de manera transparente por cuanto su uso no afecta la gestión o rendimiento. Por estas razones el cifrado en reposo es altamente recomendable.

11.3.3 Analítica y aplicaciones

Para derivar valor de los datos que provienen desde los dispositivos de IoT, las aplicaciones en la nube brindan herramientas de visualización y analítica que operan sobre fuentes o lotes de datos para identificar conocimientos adicionales. Dependiendo de caso de uso, las herramientas de gestión de decisiones y de procesos empresariales pueden desencadenar alertas o realizar acciones como respuesta.

El modelo aquí descrito propone un entorno en el que la capa Analítica y aplicaciones solo pueda acceder a los datos almacenados usando encriptación de datos, autenticación de usuario y control de acceso a la red, por cuanto es la única capa con la que tiene interés común. Es por ello que en el modelo esta capa se considera separada.

11.4 Capa de aplicación

En esta capa (Capa 4 en la figura 10, página 84) es donde se ejecutan las aplicaciones de los dispositivos, la integridad, confidencialidad y la autenticidad (CIA) de los datos deben garantizarse. En esta capa se usan protocolos como CoAP, MQTT, y AMQP que proporcionan seguridad y QoS. Para el modelo propuesto es necesario que en esta capa se implementen procesos de Autenticación adecuados para restringir el acceso de los usuarios malintencionados a los datos; Detección de intrusos que garanticen monitoreo ininterrumpido; y Seguridad de los datos mediante el cifrado, cortafuegos y software actualizados contra malwares y spywares.

la capa de aplicación interactúa con los dispositivos IoT pero no es necesario que acceda a otras capas como Data Stroage o Analisis de datos por lo que deben tomarse las medidas necesarias tendientes a proteger los datos y perpetuar la seguridad del sistema.

11.5 Fog Computing

Para enfrentar los desafíos del cifrado IoT, se propone utilizar la criptografía de curva elíptica (ECC) para asegurar la computación de niebla. La ECC proporciona longitudes de clave más cortas, tamaños de mensaje más pequeños y menor uso de recursos. La combinación de

esquemas ligeros permite una mejor escalabilidad y menos gastos de recursos que los esquemas basados en RSA empleados en SSL y TLS.

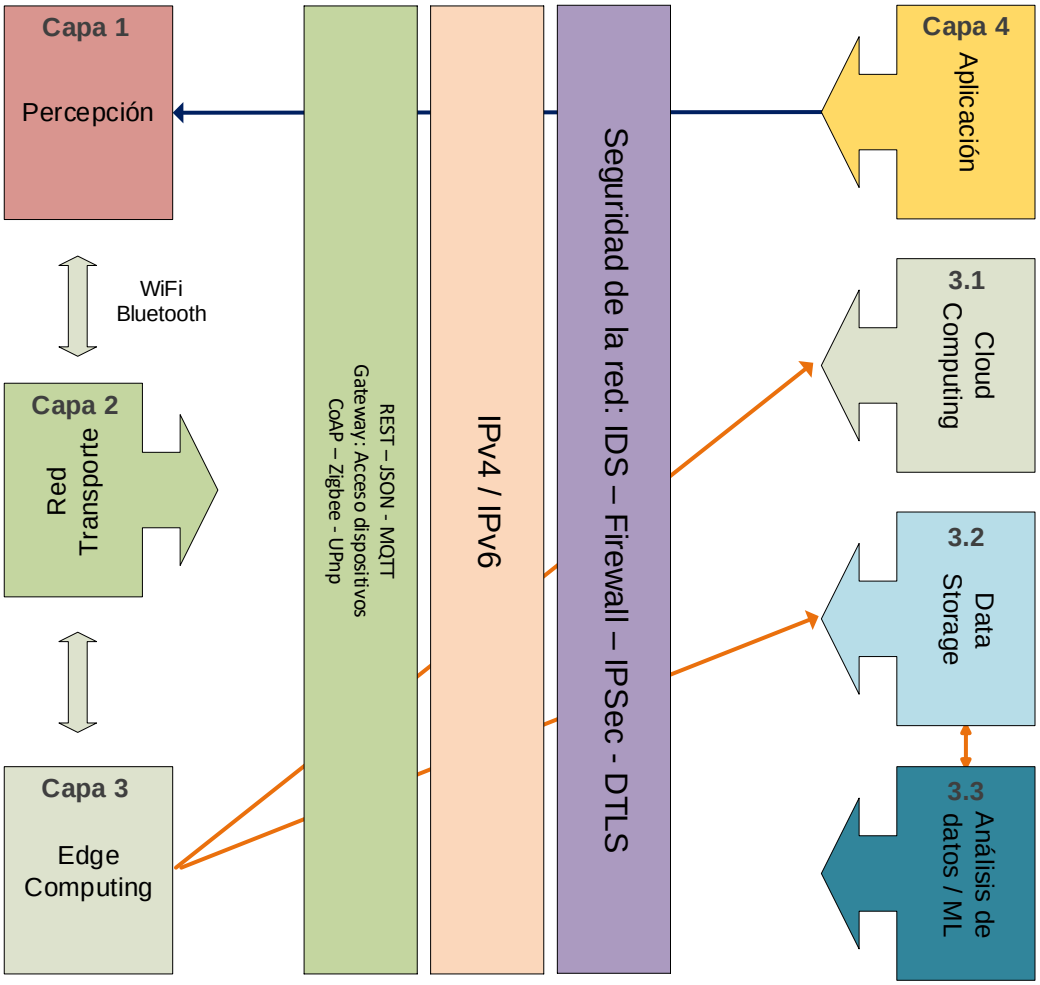

Figura 10 Arquitectura propuesta para IoT 5G
(Fuente: Elaborada por el autor)

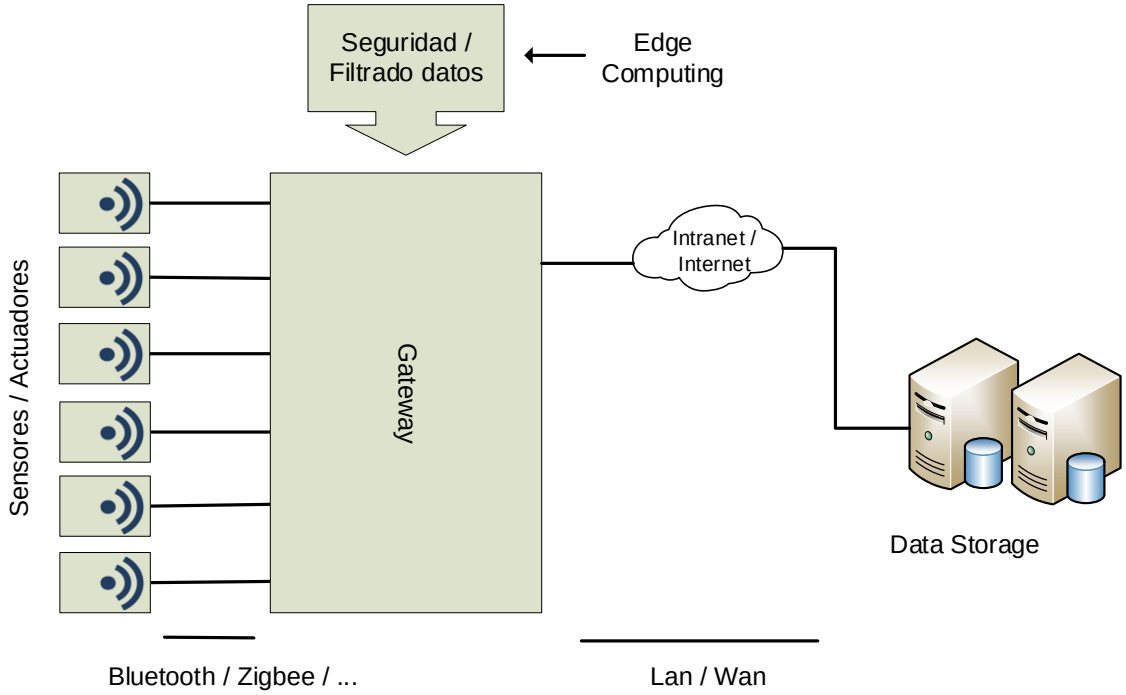

Figura 11 Modelo Edge / Gateway
(Fuente: Elaborada por el autor)

11.6 Seguridad de la red

Los objetivos de seguridad importantes de IoT son proporcionar una conexión confiable y mecanismos de autenticación adecuados y proporcionar confidencialidad sobre los datos a cada dispositivo conectado en toda la red. Las amenazas e infracciones a la CIA pueden causar daños graves al sistema y causar un impacto directo en el funcionamiento del sistema.

Aun cuando se hayan tomado todas las medidas de seguridad para el modelo incluyendo el cifrado en los dispositivos habilitados para IoT, los datos aún pueden corromperse desde dentro de las redes WSN, así como de los hosts de Internet. Por lo que es necesario la configuración de firewalls para bloquear el acceso no autorizado y un Sistema de Detección de Intrusos (IDS) para detectar impostores y actividades maliciosas en la red.

Conclusión

El marco de IoT es susceptible de ataques en cada una de las tres capas arquitectónicas; por lo tanto, hay muchos desafíos y requisitos de seguridad que deben abordarse. Existe la necesidad de nuevas tecnologías de identificación, inalámbricas, de software y de hardware para resolver los desafíos de investigación actualmente abiertos en IoT como los estándares para dispositivos heterogéneos. El estado actual de la investigación en IoT se centra principalmente en los protocolos de autenticación y control de acceso, pero con el rápido avance de la tecnología es esencial incorporar nuevos protocolos de red como IPv6 y 5G. En esta investigación, se analizaron temas de seguridad y privacidad de IoT desde una nueva perspectiva: la función IoT. Se ilustraron las más conocidas amenazas de seguridad, las soluciones existentes y los desafíos de investigación que aún deben resolverse asociados con estas características de IoT. También se ilustraron nuevas tecnologías de seguridad que requieren estudios adicionales. Finalmente, se ha propuesto un marco de seguridad que puede proporcionar autenticación y control de acceso, seguridad de red y sistema, integridad y confidencialidad utilizando las características de dicho entorno.

Trabajo futuro

A medida que IoT utiliza una arquitectura de red basada en la arquitectura de red tradicional para la comunicación entre diferentes dispositivos, se han heredado las lagunas de la arquitectura de red tradicional y también las vulnerabilidades. Deberá existir una gran necesidad de un refinamiento de la arquitectura de red existente o de crear una nueva arquitectura de red que sea liviana, efectiva y más segura, posible para resolver problemas relacionados con el rendimiento y la seguridad hasta en gran medida. Se considera necesario Implementar este modelo en un entorno industrial, agroindustrial o de salud por citar algunos ejemplos y seguir investigando para descubrir las causas fundamentales de las nuevas amenazas de seguridad de IoT y diseñar e implementar las respectivas medidas de protección.

Bibliografía

Agarwal, A. W. (2014). The Internet of Things—A survey of topics and trends. *Springer Science+Business Media*, 273.

Agrawal, S. D. (2004). *Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks.* Retrieved from https://ieeexplore.ieee.org/abstract/document/1290173

Akami. (2014). *AKAMAI'S STATE OF THE INTERNET.*

Andrés, M. B. (2018). *Internet De Las Cosas.* Madrid: Reus.

Atlam, H., Alassafi, M., Alenezi, A., Walters, R., & Wills. (2018). *XACML for Building Access Control Policies in Internet of Things.* Retrieved from https://www.researchgate.net/profile/Hany_Atlam/publication/322406219_XACML_for_Building_Access_Control_Policies_in_Internet_of_Things/links/5ac617fdaca2720544d04956/XACML-for-Building-Access-Control-Policies-in-Internet-of-Things.pdf

Atlam, H., Alenezi, A., Alharthi, A., Walters, R., & Wills, G. (2018). *Integration of Cloud Computing with Internet of Things: Challenges and Open Issues*. Retrieved from https://ieeexplore.ieee.org/abstract/document/8276823

Avast. (2018). *Avast*. Retrieved from https://www.avast.com/es-es/c-wannacry

Bai T Daisy Premila, S. A. (2015). *Elliptic Curve Cryptography based Security Framework for Internet of Things and Cloud Computing*. Retrieved from https://scholar.google.com/scholar?as_q=Elliptic+Curve+Cryptography+based+Security+Framework+for+Internet+of+Things+and+Cloud+Computing&as_occt=title&hl=en&as_sdt=0%2C31

Blog, C. (2018). *Comprobando vulnerabilidades en dispositivos Internet of Things (IoT)*. Retrieved from https://ciberseguridad.blog/comprobando-vulnerabilidades-en-dispositivos-internet-of-things-iot/

Caiming Liu, J. Y. (2011). *Research on immunity-based intrusion detection technology for the Internet of Things*. Retrieved from https://ieeexplore-ieee-org.ezproxy.utp.edu.co/document/6022060

Choi, N., Kim, D., & Lee, S. (2017). *Fog Operating System for User-Oriented IoT Services: Challenges and Research Directions*. Retrieved from https://ieeexplore.ieee.org/abstract/document/8004152

Choi, N., Kim, D., Lee, S., & Yi, Y. (2017). *Fog Operating System for User-Oriented IoT Services*. Retrieved from https://ieeexplore.ieee.org/document/8004152

Cisco. (2011). *Internet de las cosas cómo la próxima evolución de internet lo cambia todo*. Retrieved from https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342

Cisco. (2018). *Cisco*. Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cisco. (2018). Fog Computing and the Internet of Things.

CSIRT-CV. (2016). *Seguridad en Internet de las Cosas*. Retrieved from http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

Damon, R. (2003). *Applying the OSI seven layernetwork model to information security.* SANS GIAC GSEC Practical Assignment Version 1.4 b Option One.

Department for Digital Culture, U. (n.d.). *Secure by Design: Improving the cyber security of consumer Internet of Things Report.* UK.

E. Cero, J. B. (2017). *IoT's tiny steps towards 5g: Telco's perspective*. Retrieved from https://www.mdpi.com/2073-8994/9/10/213

E. Rescorla, N. M. (2006). *IEEE 802.15.4*. Retrieved from http://www.hjp.at/doc/rfc/rfc4347.html

Eset. (2017). *Eset*. Retrieved from https://noticias.eset.es/wannacry-no-fue-la-primera-amenaza-que-uso-eternalblue

Eset. (2018). *Eset Security Report Lationamérica*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

Eset. (2018). *Seguridad en dispositivos IoT: ¿Aun a tiempo de ganar la batalla?* . Retrieved from https://www.welivesecurity.com/la-es/2018/07/25/seguridad-iot-a-tiempo-ganar-batalla/

Eset. (2019). *Cómo analizar dispositivos IoT: vulnerabilidades más comunes y cómo encontrarlas*. Retrieved from https://www.welivesecurity.com/la-es/2019/01/22/como-analizar-dispositivos-iot/

españa, I. n. (2017). *Riesgos y retos de ciberseguridad y privacidad en IoT*. Retrieved from https://www.incibe-cert.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

F Bonomi, R. M. (2012). *Fog computing and its role in the internet of things*. Retrieved from https://dl.acm.org/citation.cfm?id=2342513

F. Granelli, A. A. (2015). *Software defined and virtualized wireless access in future wireless networks: scenarios and standards*. Retrieved from https://www.researchgate.net/profile/Muhammad_Usman29/publication/279246240_Soft

ware_defined_and_virtualized_wireless_access_in_future_wireless_networks_Scenarios_and_standards/links/55a7b1c808ae0b4e87126cf9/Software-defined-and-virtualized-wireless-acces

FREMANTLE, P. (2015). *A REFERENCE ARCHITECTURE FOR THE INTERNET OF THINGS*. Retrieved from https://www.researchgate.net/profile/Paul_Fremantle/publication/308647314_A_Reference_Architecture_for_the_Internet_of_Things/links/57ea00b708aef8bfcc963153.pdf

F-Secure. (2017, Junio 7). *F-Secure*. Retrieved from https://press.f-secure.com/2017/06/07/multiple-flaws-in-foscam-ip-cameras-open-devices-networks-to-attackers/

Garcia-Alfaro, J. R.-H.-M. (2016). Security of cyber-physical systems. *Proc. Conf. Security Ind. Control Cyber Phys.*

Gartner. (2017, Febrero 7). Retrieved from https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Goswami, M. I. (2013). Cloud computing: A survey on its limitations and potential solutions. *IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 2, July 2013* , (p. 161). Dhaka, Bangladesh.

Hadjichristofi, I. A. (215). Internet of Things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC).*

HakJu Kim, K. K. (2014). *Toward an Inverse-free Lightweight Encryption Scheme for IoT*. Retrieved from https://pdfs.semanticscholar.org/3484/5306ad6be9563f4d52459c2c39c45ea57127.pdf

Hernandez, G. (2104). *termostato Nest.* Retrieved from https://pdfs.semanticscholar.org/f1aa/f326c8b2cb6a94fa105b9910125e61920714.pdf

Hernandez-Castro, P. P.-L. (2006). *RFID systems: A survey on security threats and proposed solutions.* Retrieved from https://link.springer.com/chapter/10.1007/11872153_14

HP. (2014). *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack.* Retrieved from https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

hubSpot. (2019). *Seguridad del IoT: por qué se preocupan los expertos y qué puedes hacer para protegerte*. Retrieved from https://blog.hubspot.es/marketing/internet-cosas-iot-como-protegerse

Huqing Wang, N. (2014). *Study on the Improvement of ELGamal Cryptosystem Based on Elliptic Curve*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.655.9807&rep=rep1&type=pdf#page=155

I.F. Akyildiz, S. L. (2015). *Wireless software-defined networks (W-SDNs) and network function virtualization (NFV) for 5G cellular systems: An overview and qualitative evaluation*. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S1389128615003862

IBM. (2017). *Anatomía de un ataque de malware a IoT*. Retrieved from https://www.ibm.com/developerworks/ssa/library/iot-anatomy-iot-malware-attack/index.html

IEEE. (2019). *Analysis of IoT Platform Security: A Survey*. Retrieved from https://ieeexplore-ieee-org.ezproxy.utp.edu.co/document/8669423

INCIBE, I. P. (2019). *IoT: protocolos de comunicación, ataques y recomendaciones*. Retrieved from https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones

Ironpaper. (2016, Febrero 4). *Ironpaper*. Retrieved from http://www.ironpaper.com/webintel/articles/internet-of-things-market-statistics/

J Daemen, V. R. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Retrieved from https://books.google.com.co/books?hl=en&lr=&id=fNaoCAAAQBAJ&oi=fnd&pg=PA1&dq=+The+Design+of+Rijndael:+AES-the+Advanced+Encryption+Standard&ots=7iNGAFOit8&sig=Mh9eZDiEgcUlVX26hrXBIMsh5so&redir_esc=y#v=onepage&q=The%20Design%20of%20Rijndael%3A%20AES-the%20A

Jara, D. S. (2014). A survey of Internet of-things: Future vision architecture challenges and services. *2014 IEEE World Forum on Internet of Things (WF-IoT).*

Jesus Ayuso, L. M. (2010). *Optimization of Public Key Cryptography (RSA and ECC) for 16-bits Devices based on 6LoWPAN*. Retrieved from https://www.researchgate.net/profile/Antonio_Skarmeta/publication/228625830_Optimization_of_Public_Key_Cryptography_RSA_and_ECC_for_16-bits_Devices_based_on_6LoWPAN/links/544e33500cf29473161a41cb/Optimization-of-Public-Key-Cryptography-RSA-and-ECC-for-16-

Juels, A. (2006). *RFID security and privacy: a research survey*. Retrieved from https://ieeexplore-ieee-org.ezproxy.utp.edu.co/document/1589116

Jules, A. (2006). *RFID security and privacy: A research survey*. Retrieved from https://www.researchgate.net/profile/Ari_Juels/publication/3236246_RFID_security_and_privacy_A_research_survey/links/00b4953bbe80a8c975000000/RFID-security-and-privacy-A-research-survey.pdf

Kaspersky. (2017, Noviembre 17). Retrieved from https://latam.kaspersky.com/blog/kaspersky-lab-presenta-su-pronostico-de-ciberseguridad-del-2018-para-america-latina/12142/

Kaspersky. (2018, Agosto 13). *Kaspersky Lab*. Retrieved from https://latam.kaspersky.com/about/press-releases/2018_panorama-de-amenazas-phishing

Ketel, M. (2017). *Fog-Cloud Services for IoT*. Retrieved from https://dl.acm.org/citation.cfm?id=3077314

Kim, S. W. (2017). An Analysis of IoT Security Requirements And oneM2M Security Technology. *Communications of the Korean Institute of Information Scientists and Engineers.*

Lin, S., Kong, L., Gao, Q., Khan, M. K., Zhong, Z., Jin, X., & Zeng, P. (2017). *Advanced Dynamic Channel Access Strategy in Spectrum Sharing 5G Systems*. Retrieved from https://ieeexplore.ieee.org/abstract/document/8088532

Ling, J. S. (2010). Research on the architecture of Internet of Things. *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE).*

Liu, H. S. (2012). Security in the internet of things: a review. *International Conference on computer Science and Electronics Engineering (ICCSEE).*

Luan, T., Gao, L., Li, Z., Xiang, Y., Wei, G., & Sun, L. (2015). *Fog Computing: Focusing on Mobile Users at the Edge*. Retrieved from https://arxiv.org/abs/1502.01815

M. R. Palattella, M. D. (2016). *Internet of Things in the 5G Era: Enablers architecture and business models*. Retrieved from https://ieeexplore.ieee.org/abstract/document/7397856

M.R. Balasubramaniam, R. S. (2016). *an analysis of RFID authentication schemes for Internet of Things(IoT) in healthcare environment using ELgamal Elliptic Curve cryptosystem*. Retrieved from https://scholar.google.com/scholar?as_q=an+analysis+of+RFID+authentication+schemes+for+Internet+of+Things%28IoT%29+in+healthcare+environment+using+ELgamal+Elliptic+Curve+cryptosystem&as_occt=title&hl=en&as_sdt=0%2C31

Martin Hell, T. J. (2007). *Grain - A Stream Cipher for Constrained Environments*. Retrieved from https://www.cosic.esat.kuleuven.be/ecrypt/stream/p2ciphers/grain/Grain_p2.pdf

Mazhar, M. F. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computer Applications (0975 8887).*

MINSAP, D. d. (2017). *Un ciberataque global está usando una vulnerabilidad de la NSA para derribar hospitales y compañías de telecomunicaciones.* Abril. Retrieved from https://instituciones.sld.cu/dnspminsap/files/2017/05/Mayo-2017.pdf

Mosenia, A., & Jha, N. K. (2017). *A Comprehensive Study of Security of Internet-of-Things*. Retrieved from https://ieeexplore.ieee.org/document/7562568

Mukherjee, M. (2018). *Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges*. Retrieved from https://ieeexplore.ieee.org/abstract/document/8314121

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M., & Choudhury, N. (2017). *Security and Privacy in Fog Computing*. Retrieved from https://ieeexplore.ieee.org/abstract/document/8026115

Ni, J., Zhang, K., Lin, X., & Shen, X. (2017). *Securing Fog Computing for Internet of Things*. Retrieved from https://ieeexplore.ieee.org/document/8066283

Noticias, M. N. (2017). *Los mayores ciberataques de 2017 hasta la fecha*. Retrieved from https://www.pandasecurity.com/spain/mediacenter/noticias/ciberataques-hasta-la-fecha/

Org., S. (2017). *An introduction to cyber security*. Retrieved from https://www.skillsforcare.org.uk/Documents/Topics/Digital-working/An-Introduction-to-Cyber-Security.pdf

Rao, L. P. (2016). Internet of Things ─ Architecture applications security and other major challenges. *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom).*

Ray Beaulieu, D. S.-C. (2015). *Simon and Speck: Block Ciphers for the Internet of Things*. Retrieved from https://eprint.iacr.org/2015/585

Rocha, A. d. (2005). *Decentralized intrusion detection in wireless sensor networks.*

S. Raza, L. W. (2013). *SVELTE: Real-time intrusion detection in the Internet of Things*. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S1570870513001005?via%3Dihub

Samdanis, K. (2017). *5G network slicing Part I: concept principles and architectures*. Retrieved from https://ieeexplore-ieee-org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=7926919

Singh, K. D. (2014). Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack. *International Journal on Network Security.*

Statista. (2016, Noviembre 27). *Statista*. Retrieved from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Stuxnet. (2010). *Stuxnet Under the Microscope*. Retrieved from http://www.rpac.in/image/ITR%201.pdf

T. Kuo, B. L. (2018). *Deploying chains of virtual network functions: on the relation between link and server usage*. Retrieved from https://dl.acm.org/citation.cfm?id=3281123

Tuhin Borgohain, S. S. (2015). *Comparative Analysis of Cryptography Library in IoT*. Retrieved from https://arxiv.org/abs/1504.04306

Tuwanut, S. K. (2016). A SURVEY ON IOT ARCHITECTURES, PROTOCOLS, APPLICATIONS, SECURITY, PRIVACY, REAL-WORLD IMPLEMENTATION AND FUTURE TRENDS. *11th International Conference on Wireless Communications, Networking and Mobile Computing*, (p. 2). Wicom.

UIT. (2012). *Recomendación UIT-T Y.4000 / Y.2060 (2012) , 2012.*

Vaish, S. M. (2011). *Reputation-based role assignment for role-based access control in wireless sensor networks*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0140366410000885

Vaithiyanathan, M. A. (2017). *A survey on lightweight ciphers for IoT devices*. Retrieved from https://ieeexplore-ieee-org.ezproxy.utp.edu.co/document/8397271

Wagner, C. K. (2003). *Secure routing in wireless sensor networks: attacks and countermeasures*. Retrieved from https://ieeexplore-ieee-org.ezproxy.utp.edu.co/document/1203362

Wang, L. T. (2010). Future Internet: The Internet of Things. *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE).*

Weber, R. H. (2015). *Internet of things: Privacy issues revisited*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364915001156?via%3Dihub

Wei Li, W. Z. (2016). *Security Analysis of the Lightweight Cryptosystem TWINE in the Internet of Things*. Retrieved from https://scholar.google.com/scholar?as_q=Security+Analysis+of+the+Lightweight+Cryptosystem+TWINE+in+the+Internet+of+Things&as_occt=title&hl=en&as_sdt=0%2C31

X Chen, L. X.-S. (2017). *An auction-based spectrum leasing mechanism for mobile macro-femtocell networks of IoT*. Retrieved from https://www.mdpi.com/1424-8220/17/2/380

X Liu, D. H. (2017). *5G-based wideband cognitive radio system design with cooperative spectrum sensing*. Retrieved from https://www.sciencedirect.com/science/article/pii/S1874490717302483

Xinxin Fan, K. M. (2012). *WG-8: A Lightweight Stream Cipher for Resource-Constrained Smart Devices*. Retrieved from https://link.springer.com/chapter/10.1007/978-3-642-37949-9_54

Xuanxia Yaoa, Z. C. (2014). *A lightweight attribute-based encryption scheme for the Internet of Things*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167739X14002039

Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015). *Fog computing: Platform and applications*. Retrieved from https://ieeexplore.ieee.org/abstract/document/7372286

Yiyuan Luo, Q. C. (2010). *A Lightweight Stream Cipher WG-7 for RF Encryption and Authentication*. Retrieved from https://ieeexplore.ieee.org/abstract/document/5684215

Zaheer, R. K. (2012). *Future internet: the internet of things architecture, possible applications and key challenges.* Retrieved from https://ieeexplore.ieee.org/abstract/document/6424332

Zheng Gong, S. N. (2012). *KLEIN: A New Family of Lightweight Block Ciphers*. Retrieved from https://link.springer.com/chapter/10.1007/978-3-642-25286-0_1